



LAUREA
AMMATTIKORKEAKOULU

Uuden edellä

Espoon kaupungin kameravalvonnan kehittäminen

Kuusela, Timo

2012 Laurea Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Espoon kaupungin kameravalvonnan kehittäminen

Timo Kuusela
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu, 2012

Sisällys

1	Johdanto	6
2	Keskeiset käsitteet ja aiempi tutkimus	6
2.1	Kameravalvonta	6
2.2	Valvomo	7
2.3	Aiempi tutkimus	7
2.4	Johdanto kameravalvontaan	8
3	Kohdeorganisaatio ja laitteiston nykytila	8
4	Lainsäädäntö	9
4.1	Laki yksityisyyden suojasta työelämässä	10
4.2	Henkilötietolaki	12
4.3	Työturvallisuuslaki	13
4.4	Rikoslaki	13
5	Kameratekniikka, etävalvonnan haasteet	14
5.1	Analogitekniikan edut ja haitat	15
5.2	Digitaalitekniikan edut ja haitat	15
5.3	Hybriditekniikka	19
5.4	Muut tekninen kehitys	19
5.5	Tietoturva	20
5.6	Etävalvonnan haasteet	21
5.7	Valvomo	24
6	Kehittämisehdotukset, jatkotutkimus, työn arviointi	27
6.1	Jatkotutkimuskohteet	28
6.2	Opinnäytetyön arviointi	29
7	Yhteenveto	30
	Lähteet	31

Timo Kuusela

Espoon kaupungin kameravalvonnan kehittäminen

Vuosi	2012	Sivumäärä	33
-------	------	-----------	----

Tässä opinnäytetyössä käsitellään Espoon kaupungin sosiaali- ja terveystoimen kameravalvontajärjestelmän nykytilaa, sekä tuodaan esille millaisia asioita järjestelmän kehittämisessä tulevaisuudessa tulisi huomioida. Nykyisellään kaupungin sosiaali- ja terveystoimella on yhteensä 442 kameraa 37 eri kohteessa. Kameravalvonnan kamerat eivät ole tällä hetkellä yhdistettynä keskitettyyn valvomoon vaan jokaisen tallentimet sijaitsevat kohteessa ja valvonta suoritetaan henkilökunnan toimesta. Kaupungin sosiaali- ja terveystoimen kameravalvonta on tulevaisuudessa tarkoitus yhdistää yhden keskitetyn valvomon alle, nykyisen kohdekohtaisesti valvotun järjestelmän sijasta. Yhdistäessä näin suurta määrää kameroita yhdeksi kokonaisuudeksi, tulee esille hyvin monenlaisia asioita joita järjestelmää kehittäessä tulee huomioida.

Opinnäytetyössä käsitellään suuren kameravalvontajärjestelmä kehittämisen haasteita niin lainsäädännön, kameratekniikan, tallennintekniikan, tietoturvan, etävalvonnan haasteiden sekä keskitetyn valvomon näkökulmasta. Työssä annetaan kehittämis ehdotuksia siihen, millaisia asioita suurta kameravalvontajärjestelmää keskittäessä sekä kehittäessä tulisi huomioida. Opinnäytetyö ei sinällään anna minkäänlaista tarkkaa määritelmää siitä, millainen järjestelmä olisi kaikista paras mahdollinen, vaan kuvaa erilaisien vaihtoehtojen hyviä sekä huonoja puolia. Käytännössä toteutettavaan järjestelmään tulevat vaikuttamaan erilaiset tekijät kuten budjetti sekä valvonnan tyyppi, joten kovin täsmällisten ohjeiden antaminen toteuttamiseen ei ole tässä opinnäytetyössä tarkoituksenmukaista.

Työssä käsitellään myös joitain sellaisia tekniikkaan, valvomon keskittämiseen ja tietoturvasuuteen liittyviä asioita, joihin ei tässä työssä suoranaisia kehittämis ehdotuksia pysty antamaan. Muun muassa kohdistettuihin hyökkäyksiin, tallentimien tietoturvaan ja keskitetyn valvomon etuihin sekä haittoihin viitataan työssä. Nämä asiat olisi hyvä huomioida suurta kameravalvontajärjestelmää toteuttaessa, mutta opinnäytetyössä käsiteltyjen tietojen perusteella niistä ei voi antaa järin vahvoja suosituksia. Kyseisiä asioita olisikin hyvä tutkia pidemmälle, esimerkiksi opinnäytetyön muodossa.

Timo Kuusela

CCTV system development in the city of Espoo

Year	2012	Pages	33
------	------	-------	----

This thesis analyzes the current state of the CCTV system (closed-circuit television) in Espoo's Social and Health services and gives statements on how to develop the system in future. The thesis describes what should be considered when the system will be transferred into centralized monitoring and storage. Currently the Social and Health services sector has a total of 442 cameras in 37 different locations. The cameras are monitored locally only and there is no centralized monitoring, management or storage. Monitoring of CCTV cameras is performed by staff along with their other work duties. In the future the CCTV system will be centrally monitored, which will require that multiple factors are taken into account.

This thesis describes the challenges faced during large centralization project such as this. The challenges arise from for example complex legislation, changes in camera technology, different video recorder technologies, information security issues and generally from centralizing a large number of cameras into a single monitoring centre. This thesis does not give any exact recommendation on how to centralize a CCTV system but rather indicates the upsides and downsides of different types of implementation. Based on those points some recommendations are given on how certain matters could be arranged. In reality such aspects as such as for example budget and the type of monitoring done on the camera system define which system is implemented. Due to these factors it's not possible for me to say exactly how to build the system.

This thesis also discusses issues regarding camera technology, centralized monitoring and information security on which strong recommendations cannot be given. For example targeted attacks, security of digital CCTV video recorders and the benefits and downsides of centralized monitoring are only briefly described in the thesis. In any case these aspects should be considered when centralizing a large CCTV system such as is described in this thesis. Further investigation into these issues should be conducted by someone for example in form of a thesis.

Keywords CCTV, development, centralized, monitoring, camera technology

1 Johdanto

Opinnäytetyön idea tuli minulle Espoon kaupungilta. Turvallisuussuunnittelija Veli-Pekka Hytinen ehdotti, että tekisin kaupungin sosiaali- ja terveystoimen kameravalvontaan liittyvän opinnäytetyön. Siinä olisi tarkoitus kartoittaa, millaisia järjestelmiä kaupungilla on tällä hetkellä olemassa ja minkälaisia toimenpiteitä kaikkien kohteiden valvominen keskitetystä valvomosta vaatisi. Järjestelmät tullaan tulevaisuudessa mahdollisesti yhdistämään niin, että koko Espoon kaupungin kameravalvonta on keskitettynä yhdeksi kokonaisuudeksi. Nykyisellään esimerkiksi sosiaali- ja terveystoimessa jokaisen kohteen omat työntekijät hoitavat valvomisen. Koska kameravalvontajärjestelmät ovat eri-ikäisiä ja ne ovat toteutettu eri toimipisteiden tarpeiden mukaisesti, on laitteisto nykyisellään varsin hajanaista. Työlle on siis olemassa todellinen tarve, sillä mikäli mahdollinen yhdistäminen joskus toteutetaan, täytyy järjestelmän eri laitteet ja niiden yhdistämisen vaatimukset joka tapauksessa selvittää.

2 Keskeiset käsitteet ja aiempi tutkimus

Opinnäytetyön kannalta keskeisimmät käsitteet on kuvattu tässä luvussa. Käsitteet antavat osaltaan kuvaa siitä, mikä työn keskeinen sisältö on sekä auttavat välttämään väärinkäsityksiä. Luvussa käsitellään myös kameravalvontaan liittyvää aikaisempaa tutkimusta. Aikaisemman tutkimuksen tuloksista on tarkoitus saada työhön jonkinlaista näkökulmaa siitä, millainen urakka ison kameravalvontajärjestelmän kehittäminen on. Viimeisenä tässä osiossa käsitellään lyhyesti kameravalvonnan nykytilaa.

2.1 Kameravalvonta

Finanssialan keskusliiton määritelmän mukaan kameravalvonnalla tarkoitetaan sellaista laitteistoa, jolla tuotetaan jatkuvaa kuvallista informaatiota kiinteistöstä tai siellä liikkuvista henkilöistä. Valvonnassa tuotettu informaatio voidaan tallentaa ja sitä voidaan käyttää tapahtumien reaaliaikaiseen valvomiseen. Määritelmän mukaan kameravalvonnalla on myös tarkoitus antaa tietoa, jolla voidaan välttää omaisuus- tai henkilövahinkojen syntymistä. (Kameravalvonnan K-menetelmä 2006, 5.) Laki yksityisyyden suojasta työelämässä määrittelee kameravalvonnan jokseenkin samalla tavalla todeten kameravalvonnan olevan ”jatkuvasti kuvaa välittävän tai kuvaa tallentavan teknisen laitteen käyttöön perustuvaa valvontaa” (Laki yksityisyyden suojasta työelämässä 13.8.2004/759). Tässä opinnäytetyössä kameravalvonnalla tarkoitetaan sellaista teknistä järjestelmää, jossa kameroiden ja tallentimen avulla sekä kaapataan että samanaikaisesti tallennetaan videokuvaa tietyssä kohteessa. Tässä opinnäytetyössä ei käsitellä kameravalvontajärjestelmiä, joita käytetään pelkästään kohteen valvomiseen eikä ollenkaan tallentamiseen.

2.2 Valvomo

Kameravalvontaoppaan määritelmän mukaan valvomolla tarkoitetaan aktiivisessa kameravalvonnassa keskusta, joka ottaa vastaan kamerakuvat sekä muut mahdolliset hälytystiedot. Valvomossa tarkkaillaan kameroiden kaappaamaa valvontakuvaa monitoreista sekä tarvittaessa ohjataan käännettäviä kameroita. Valvomossa tehdään tapahtumien sekä hälytyksien perusteella tilannearvioita ja tarvittaessa käynnistetään toimenpiteitä vahinkojen välttämiseksi. (Sallinen ym, 38.) Finanssialan keskusliitto määrittelee puolestaan valvomon tilana, jonka tarkoitus on ”vastaanottaa kiinteistöistä saapuvaa kamerakuvaa ja informaatiota, tehdä tilannearvioita, käynnistää kameravalvontasuunnitelman ja palvelusopimuksen mukaisia toimenpiteitä ja ylläpitää tarvittavia kiinteistötietoja” (Kameravalvonnan K-menetelmä 2006, 26.) Tässä opinnäytetyössä valvomolla tarkoitetaan sellaista kahden yllä mainitun kuvauksen mukaista keskusta, jossa kamerakuvaa tarkkaillaan ja sen perusteella tehdään päätöksiä. Vielä tarkemmin kuvattuna valvomo on tässä työssä sellainen keskitetty valvomo, jossa tarkkaillaan useamman kohteen tuottamaa kameravalvontakuvaa. Sanalla valvomo ei siis työssä viitata sellaiseen tilaan, jossa tarkkaillaan ainoastaan kyseisen kohteen tuottamaa valvontakamerakuvaa.

2.3 Aiempi tutkimus

Vähänkään suuremman kameravalvontajärjestelmän kehittämisestä ei ollut kovin helposti löydettävissä tietolähteitä. Suurin osa kameravalvonnan kehittämiseen liittyvistä teksteistä oli tehty huomattavasti pienempiin kohteisiin. Erittäin isojen kameravalvontajärjestelmien kehittämisestä sekä luomisesta ei juuri löydy julkista tietoa Internetistä. Jotkin päivityksiin liittyvät työt ovat tyyliltään selkeästi teknisempiä ja niissä perehdytään hyvin yksityiskohtaisesti järjestelmän tekniikan yksityiskohtiin, kuten videokuvan eri pakkausmenetelmiin sekä muihin vastaaviin tietoihin.

Britanniassa, jossa kameravalvontaa on erittäin paljon, on myös julkaistu useita tutkimuksia etenkin julkisen kameravalvonnan tehokkuudesta. Näistä tutkimuksista on kuitenkin hankala löytää sellaista, joka olisi tehty yksittäisen rakennuksen kameravalvonnan tehokkuudesta. Monien tutkimuksien kameravalvontajärjestelmät ovat viranomaiskäyttöön tarkoitettuja ja julkisten alueiden valvomiseen käytettyjä. Tutkimuksista ei tämän vuoksi ole mahdollista saada kovin hyvää kuvaa siitä, kuinka tehokasta kameravalvonta on yksittäisessä rakennuksessa esimerkiksi rikollisuuden vähentämiseen. Eräässä tutkimuksessa kuitenkin todettiin, että kameravalvonta julkisillakin paikoilla toimii kaikista parhaiten pienillä ja suljetuilla alueilla.

2.4 Johdanto kameravalvontaan

Kameravalvonnan käyttö erilaisissa tilanteissa ja kohteissa on lisääntynyt viime vuosina ja siitä on tullut osa normaalia arkea monessa paikassa. Kameravalvontaa käytetään etenkin rikosten selvittämiseen sekä pelotevaikutuksensa vuoksi myös rikostentorjuntaan. Erityisen hyödyllinen kameravalvonta on erilaisten tapahtuneiden rikosten sekä muiden haitallisten tapahtumien selvittämiseen, sillä valvontakameroiden tallentamasta kuvamateriaalista voidaan nähdä parhaimmillaan selkeästi ja puolueettomasti, mitä tilanteessa on todellisuudessa tapahtunut. Oikein toteutettuna kameravalvonnan avulla voidaan parantaa organisaation häiriöttömän toiminnan jatkuvuutta. Monesti myös poliisi käyttää kameravalvontaa omiin tarkoituksiinsa, esimerkiksi Suomessa yleisen järjestyksen ja turvallisuuden ylläpitämiseen poliisilain mukaisesti sekä liikennevalojen ja liikennevirtojen ohjaamiseen. (Sallinen ym, 6.)

Vaikka kameravalvontaa käytetään yleisesti rikostorjunnan yhtenä keinona, ei tutkimuksilla ole pystytty todistamaan, vähentääkö kameravalvonta rikollisuutta julkisilla paikoilla vai siirtääkö valvonta rikollisuuden ainoastaan muualle. Moni kameravalvonnan tehokkuutta koskevista tutkimuksista on tullut lopputulokseen, ettei kameravalvonnan rikoksia vähentävää vaikutusta voida varmasti näyttää toteen. Eräiden tutkimusten mukaan esimerkiksi jopa valaistuksen lisäämisellä julkisilla paikoilla on kameravalvontaa huomattavasti suurempi vaikutus omaisuusrikollisuuden vähenemiseen. (Harris & Harris, 2009.) Britanniassa suoritetun tutkimuksen mukaan kameravalvonta julkisilla paikoilla on kaikista tehokkainta rikollisuuden torjunnassa, mikäli alue on kooltaan pieni ja suljettu (Gill & Spriggs 2005, 117).

Toisaalta näkökulma kameravalvonnan tehokkuudesta yksityisellä alueilla poikkeaa huomattavasti julkisten ulkoalueiden kameravalvonnan tehokkuudesta. Yksityisellä puolella kameravalvontaa käytetään monesti selvittämään ja ratkaisemaan jo tapahtuneita rikoksia ja täten sitä pidetään rikostorjunnan kannalta kannattavana. (Honovich, 2008.) Myös Hannu Huuhtasen eri yritysten liikejohdolle tekemän kyselyn mukaan kameravalvonta on erityisesti hyödyllistä tapahtuneiden tilanteiden todentamiseen sekä ulkoisen varkaushävikin vähentämiseen (Huuhtanen 2009, 100). Kameravalvonnasta on siis etenkin hyötyä, mikäli pyritään selvittämään jo tapahtuneita tilanteita, sillä kameravalvonnalla saadaan puolueeton näkökulma sekä konkreettista videokuvaa tapahtuneesta tilanteesta.

3 Kohdeorganisaatio ja laitteiston nykytila

Espoon kaupungin organisaatio on jakautunut neljään osaan, jotka ovat sosiaali- ja terveystoimi, sivistystoimi, tekninen ja ympäristötoimi sekä palveluliiketoimi. Opinnäytetyössä käsiteltävän sosiaali- ja terveystoimen viranhaltijaorganisaatiota johtaa perusturvajohtaja. Hänen

alaisuudessaan on toimialan esikunta, sisäinen tarkastus sekä konsernipalveluiden yksikkö. Näiden kolmen alapuolella ovat toimialan eri tulosityksiköt. Vuonna 2011 sosiaali- ja terveys-toimi rakentuu kolmesta tulosityksiköstä, jotka ovat perhe- ja sosiaalipalveluiden, terveystalveluiden sekä vanhuspalvelujen tulosityksiköt. Espoon kaupungin sosiaali- ja terveystoimi tuottaa terveys-, perhe-, sosiaali- sekä vanhuspalveluita ja työntekijöitä on 3 300 kappaletta. (Espoon kaupunki 2011a, 2011b.)

Nykyisellään Espoon kaupungin sosiaali- ja terveystoimen kameravalvonnan laitteisto koostuu hyvin monen valmistajan eri tuotteista. Kaikki järjestelmien kamerat ovat yhtä kohdetta lu-kuun ottamatta analogisia, eivätkä kohteista kaikki ole nykyisellään liitettävissä etävalvon-taan. Järjestelmän kohdekohtaiset toteutuserot tuovat haastetta sen kehittämiseen sekä val-vonnan keskittämiseen. Espoon kaupungin sosiaali- ja terveystoimella on tällä hetkellä yh-teensä 26 kameravalvottua kohdetta. Ne ovat enimmäkseen eri kaupunginosien terveysase-mia, hammashoitoloita sekä sosiaalitoimistoja tai lastensuojelun tiloja. Kameroita on yhteen-sä 442, mikä tuo oman haasteensa kaikkien tilojen keskitettyyn valvontaan. Tallentimia jär-jestelmässä on yhteensä 37 ja kaikki tallentimet sijaitsevat kohdekiinteistöissä kyseisen kiin-teistön kannalta sopivimmassa tilassa. Jos kohteessa on oma vahtimestari, valvoo hän työnsä ohessa tarvittaessa valvontakameroita. Kaupungilla on myös kohteita, joissa kameroilla ei ole minkäänlaista jatkuvaa valvontaa. Näissä tiloissa kameroiden tallentamaa videokuvaa katso-taan ainoastaan, mikäli tiloissa on tapahtunut jotakin, minkä selvittämiseen kameravalvonnan materiaali mahdollisesti tuo apua.

4 Lainsäädäntö

Kameravalvontaa koskevan lainsäädännön ongelmana on sen hajaantuminen erittäin moneen lakiin. Joissain laeissa saattaa olla vain joitain hyvin lyhyitä ja yksittäisiä pykälä, jotka kos-kevat kameravalvontaa vain tietyissä tilanteissa. Tämä tekee kameravalvontaa koskevan lain-säädännön kokonaisuuden käsittämisen haastavammaksi, kuin se olisi tilanteessa, jossa kaikki kameravalvontaa sisältävä lainsäädäntö olisi yhdessä omassa laissaan. Kameravalvontaa kos-kee kuusi eri lakia, jotka ovat lueteltuna alla.

- Rikoslaki (39/1889)
- Laki yksityisistä turvallisuuspalveluista (282/2002)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki yhteistoiminnasta yrityksissä (334/2007)
- HTL henkilötietolaki (523/1999)
- TTL työturvallisuuslaki (738/2002)

Laki yhteistoiminnasta yrityksissä sekä laki yksityisistä turvallisuuspalveluista eivät kosketa tämän opinnäytetyön kohdetta. Lain yhteistoiminnasta yrityksissä neljäs pykälä mainitsee, ettei laki päde mikäli kohde on kunnan tai kuntayhtymän virasto. (Laki yhteistoiminnasta yrityksissä 334/2007.) Laki työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnista puolestaan ei mainitse mitään yhteistoiminnan tarpeesta kameravalvontaa tai muuta valvontaa toteuttaessa. Laki yksityisyyden suojasta työelämässä mainitsee kuitenkin, että kameravalvonnan toteuttaminen kuuluu yhteistoiminnan piiriin myös kunnan tapauksessa (Laki yksityisyyden suojasta työelämässä 759/2004). Koska kaikki kamerat ovat tällä hetkellä kaupungin oman hallinnan alla, eikä niiden valvomista ole tilattu vartiointiliikkeeltä, ei lakia yksityisistä turvallisuuspalveluista käsitellä opinnäytetyössä.

4.1 Laki yksityisyyden suojasta työelämässä

Laki yksityisyyden suojasta työelämässä sisältää oman lukunsa kameravalvonnan käytöstä työpaikoilla. Lain viidennessä luvussa määritellään muun muassa, millaisissa tiloissa kameravalvontaa saa käyttää. Laki sisältää myös tietoa siitä, kuinka kameravalvonnan avoimuus tulee järjestää valvontaa toteutettaessa.

Lain 16 § ilmaisee, mihin asioihin joko kuvaa välittävää sekä kuvaa tallentavaa kameravalvontaa saadaan käyttää työpaikalla. Kameravalvontaa saadaan käyttää työpaikalla ensinnäkin tiloissa työskentelevien sekä siellä oleskelevien henkilöiden turvallisuuden varmistamiseksi. Samoin kuin henkilöiden turvallisuuden varmistamiseen voidaan lain mukaan kameravalvontaa käyttää myös omaisuuden suojaamiseen tai tuotantoprosessin asianmukaisen toiminnan varmistamiseen. Kolmanneksi laki mainitsee, että kameravalvontaa voidaan käyttää myös turvallisuutta, omaisuutta tai tuotantoprosessia vaarantavien tilanteiden ennaltaehkäisyyn tai niiden selvittämiseen. Kameravalvontaa työpaikalla ei lain 16 §:n mukaan kuitenkaan saa käyttää ensinnäkään jonkin henkilön tai henkilöiden tarkkailuun työpaikalla. Toiseksi laki mainitsee, ettei käymälässä, pukeutumistilassa tai näitä vastaavassa tilassa eikä henkilökohtaisen käyttöön osoitetussa työhuoneessa saa käyttää kameravalvontaa. Poikkeuksia edellisiin kieltoihin määritellään lain 16 §:ssä tilanteisiin, joissa kameravalvonta on välttämätöntä tietyssä työpisteessä. Kameravalvonnan välttämättömyydelle voi ensinnäkin olla perusteena työntekijän työhön liittyvä ilmeinen väkivallan uhka, uhka hänen turvallisuudelleen tai terveydelle ilmeisen haitan ehkäisemiseen. Toisekseen kameravalvontaa voidaan kohdistaa työpisteeseen, jos työntekijän työnkuvaan kuuluu olennaisena osana arvoltaan tai laadultaan merkittävän omaisuuden käsittely. Näitä ovat lain mukaan esimerkiksi raha, arvopaperit tai arvoesineet. Tällaisissa tilanteissa kameravalvontaa saadaan käyttää, mikäli valvonnalla pyritään ehkäisemään tai selvittämään omaisuuteen kohdistuvia rikoksia. Viimeksi lain 16 §:ssä mainitaan, että kameravalvontaa voidaan käyttää työntekijän etujen ja oikeuksien varmistamiseen. Tämä

valvonta vaatii kuitenkin tarkkailun kohteeksi tulevan työntekijän pyyntöä, ja asiasta tulee sopia työnantajan ja työntekijän välillä. (Laki yksityisyyden suojasta työelämässä 759/2004.)

Lain 17 § käsittelee kameravalvonnan suunnittelun ja toteutuksen aikana vaadittua avoimuutta. Ensinnäkin laki määrittää, että työnantajan on ennen kameravalvonnan käyttöönottoa selvitettävä muiden, vähemmän työntekijöiden yksityisyyteen puuttuvien keinojen käyttömahdollisuudet. Toisekseen laki määrittää, että työntekijän yksityisyyteen ei puututa yhtään enempää kuin toimenpiteiden tarkoituksen saavuttamiseksi on välttämätöntä. Kolmantena asiana laki toteaa, että kameravalvonnalla luodut henkilöitä koskevat tallenteet tulee käsitellä henkilötietolain vaatimusten mukaisesti. Henkilötietolaki käsittelee näitä vaatimuksia 5-7, 10 ja 32-34 §:ssä. Henkilötietolain pykälää tulee noudattaa, vaikkei tallenteista syntyisikään henkilötietolaissa määriteltyä henkilörekisteriä. Kameravalvontamateriaalia tulee lain mukaan käyttää pelkästään niihin tarkoituksiin, joita varten tarkkailu kameravalvonnalla on toteutettu. Kameravalvonnasta on lain 17 § mukaan ilmoitettava näkyvällä tavalla niissä tiloissa, joissa on kameroita. (Laki yksityisyyden suojasta työelämässä.)

Aikaisemmin määriteltyjen kohtien lisäksi kameravalvontaa saadaan lain 17 §:n mukaan ensinnäkin käyttää työsuhteen päättämiseen tarvittavan perusteen toteennäyttämiseen. Toisekseen kameravalvontaa voidaan käyttää tasa-arvolaisissa tai työturvallisuuslaissa kuvatun mukaisen häirinnän tai epäasiallisen käytöksen selvittämiseen ja toteen näyttämiseen. Häirinnän selvittäminen vaatii kuitenkin työnantajalta perustellun syyn epäillä, että tarkkailtava henkilö todella on syylistynyt häirintään. Lisäksi kameravalvontaa voidaan käyttää työtapaturman tai työturvallisuuslaissa kuvatunlaisen vaaraa tai uhkaa aiheuttaneen tilanteen selvittämiseksi. (Laki yksityisyyden suojasta työelämässä)

Kameravalvonnalla tuotetut tallenteet tulee lain mukaan tuhota viimeistään vuoden kuluttua tallentamisen päättymisestä, mikäli muita pidempään säilyttämiseen oikeuttavia tekijöitä ei ole. (Laki yksityisyyden suojasta työelämässä.) Pidempään säilyttämiseen oikeuttaa häirintään, työtapaturmiin, vaara- ja uhkatilanteisiin sekä työsuhteeseen päättämiseen liittyvien asioiden selvittäminen. Tämä edellyttää kuitenkin, että kameravalvonnan tallenne on oleellinen asian selvittämisen kannalta. (Sallinen ym, 58.) Mikäli kameravalvonnan toteuttamista tai avoimuutta koskettavia säännöksiä rikotaan, voidaan työnantaja tai tämän edustaja tuomita yksityisyyden suojasta työelämästä annetun lain rikkomisesta sakkoon. Kameravalvonnan ollessa kyseessä voidaan antaa tuomio myös salakatselusta. (Laki yksityisyyden suojasta työelämässä.)

4.2 Henkilötietolaki

Tietosuojavaltuutetun toimiston (2011) mukaan kameravalvonnan tallentamat kuva ja ääni täyttävät henkilötietolain määrittämisen henkilötiedoista, joten lain vaatimuksia on noudatettava toteuttaessa kameravalvontaa. Lain mukaan henkilötietojen käsittelyä on tiedon kerääminen, tallentaminen, järjestäminen, käyttö, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen, tuhoaminen sekä muut henkilötietoihin kohdistuvat toimenpiteet. Henkilötietolain toisen luvun 10 § määrittää että, rekisterinpitäjän on laadittava henkilörekisteristä rekisteriseloste. Siitä on käytävä ilmi rekisterinpitäjän tai tarvittaessa tämän edustajan nimi ja yhteystiedot, tarkoitus henkilötietojen käsittelylle, kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä, tieto siitä, mihin tietoja luovutetaan sekä kuvaus rekisterin suojauksen periaatteista. Rekisteriseloste on oltava kaikkien saatavilla. (Henkilötietolaki 523/1999.) Kameravalvonnan ollessa kyseessä rekisteriselosteen julkisuudesta voidaan kuitenkin poiketa, mikäli se on välttämätöntä valtion turvallisuuden, puolustamisen tai yleisen järjestyksen ja turvallisuuden vuoksi sekä mikäli se on välttämätöntä, jotta voidaan ehkäistä tai selvittää rikoksia. Oleellisin asia henkilötietolaissa on kameravalvonnan kannalta rekisteriselosteen luominen järjestelmälle. (Sallinen ym, 59-60.)

Rangaistukset henkilörekisteriin liittyvistä rikoksista ovat rikoslain 10. luvun 9 §:ssä. Mikäli henkilö rikkoo henkilötietolakia, voidaan hänet tuomita henkilörekisteririkkomuksesta sakkoon, jollei rikoksesta ole jossain muussa laissa ankarampaa rangaistusta. Henkilötietolaissa on neljä eri seikkaa, joiden laiminlyönnistä voidaan rikoslain mukaan tuomita. Ensimmäisenä laissa on mainittu rekisteriselosteeseen liittyvät rikkomukset, jotka koskevat tietojen käsittelyä vastoin niitä määräyksiä, joita henkilötietolaissa on asetettu käyttötarkoitussidonnaisuudesta, käsittelyn yleisistä edellytyksistä, henkilötietojen tarpeellisuudesta tai virheettömyydestä, arkaluonteisten tietojen, henkilötunnuksien tai henkilötietojen käsittelystä erityisiä tarkoituksia varten. Ensimmäisessä kohdassa mainitaan rangaistavana asiana myös henkilötietojen käsittely vastoin henkilötietojen käsittelyä koskevia erityissäännöksiä. Toiseksi rikoslain mukaan henkilötietolakiin liittyvästä rikoksesta voidaan tuomita henkilö, joka antaa tietosuojaviranomaiselle väärän tai harhaanjohtavan tiedon henkilötietojen käsittelyä koskevassa asiassa. Kolmanneksi rikoslain mukaan henkilörekisteririkkomuksesta voidaan tuomita henkilö, joka rikkoo säännöksiä tai määräyksiä, jotka koskevat henkilötietojen suojaamista sekä henkilörekisterin hävittämistä. Viimeinen henkilötietolakiin liittyvä rangaistukseen johtava teko on tietosuojalautakunnan antaman lainvoimaisen määräyksen rikkominen. (Rikoslaki.)

4.3 Työturvallisuuslaki

Työturvallisuuslain viidennen luvun 27 § mainitsee, että sellaisessa työssä, johon liittyy ilmeinen väkivallan uhka, on työ ja työolosuhteet järjestettävä niin, että uhka- ja väkivaltatilanteet mahdollisuuksien mukaan ehkäistään etukäteen. Laki tarkentaa vielä, että työpaikalla on tällaisessa tilanteessa oltava tarvittavat laitteistot ja turvallisuusjärjestelyt väkivallan torjumiseen tai rajoittamiseen sekä mahdollisuus avun hälyttämiseen. Työnantaja on myös vastuussa siitä, että olemassa olevat turvallisuusjärjestelyt sekä laitteet todellisuudessa myös toimivat. (Työturvallisuuslaki 738/2002.) Kameravalvontaa voidaan pitää sellaisena työturvallisuuden keinona, jota käytetään työssä mahdollisesti esiintyvän väkivallan ehkäisemiseen. Mikäli kohteessa jonkin tilan turvallisuudesta varmistutaan nimenomaan kameravalvontakuvan perusteella, on kameravalvonta keskeinen osa työturvallisuutta. Jos kameravalvonta on kohteen turvallisuuden kannalta oleellinen, voidaan sen hoidon laiminlyönnistä tuomita lain mukaan rangaistukseen. Rangaistus voi olla joko työturvallisuuslain 8 luvun 63 §:n työturvallisuusrikkomuksen tai rikoslain 47 luvun 1 §:n työturvallisuusrikoksen mukainen. Rikoslaisissa mainitaan, että työturvallisuusrikoksesta voidaan tuomita sakkoon tai enintään vuodeksi vankeuteen sellainen työnantaja tai työnantajan edustaja, joka tahallaan tai huolimattomuudestaan jättää noudattamatta työturvallisuusmääräyksiä tai työsuojelun edellytyksiä. (Sallinen ym, 58-59.)

4.4 Rikoslaki

Rikoslaisissa kameravalvonnan kannalta oleelliset säädökset koskevat salakatselua. Mikäli kameravalvonta on toteutettu huolimattomasti, saatetaan sillä pahimmillaan syyllistyä salakatseluun. Rikoslain mukaan salakatselua on sellainen toiminta, jossa teknisellä laitteella katsellaan tai kuvataan henkilöä, joka oleskelee kotirauhan suojaamassa paikassa, käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa. (Rikoslaki 39/1889.) Käymälää tai pukeutumistilaa vastaavia huoneita ovat esimerkiksi pukuhuoneet ja saunat, joissa henkilö voi olettaa olevansa turvassa ulkopuolisten katseelta ja kuvaamiselta niissä suoritettavien toimien intiimiyden vuoksi. Henkilön kuvaaminen ei kuitenkaan ole salakatselua kotirauhan suojaamassa paikassa, mikäli esimerkiksi omakotitalon omistaja tallentaa kuvaa hänen taloonsa luvattomasti tunkeutuneesta henkilöstä. Kameravalvontaoppaan mukaan teknisellä laitteella tarkoitetaan yleensä kiikareita, kameroita videokameroita sekä muita edellä lueteltuihin rinnastettavia laitteita. (Sallinen ym, 51-52.)

Toiseksi rikoslaisissa mainitaan että salakatselua on myös toiminta, jossa henkilön yksityisyyttä loukaten katsellaan tai kuvataan henkilöä, joka oleskelee yleisöltä suljetussa rakennuksessa, huoneistossa tai aidatulla piha-alueella. Tarkemmin tämän merkistön täyttävät tilat on lueteltu rikoslain 24. luvun julkisrauhan rikkomista käsittelevässä kolmannessa pykälässä. Rikoslain

24. luvun kolmas pykälä mainitsee, että tällaisia tiloja ovat virastot, liikehuoneistot, toimitukset, tuotantolaitokset, kokoustilat tai muut vastaavat huoneistot tai rakennukset, rakennuksen aidatut piha-alueet, kasarmialueet, puolustusvoimien tai rajavartiolaitoksen käytössä olevat alueet, joissa asiaton liikkuminen on kielletty. (Rikoslaki 39/1889.)

Huomioitavaa on myös, että jo pelkkä salakuuntelun tai salakatselun valmistelu on lain mukaan rangaistavaa. (Rikoslaki 39/1889.) Salakatselua ei kuitenkaan ole pelkkä jonkin tietyn tilan, eläinten, esineiden, rakennuksien tai muun ympäristön tallentaminen tai katseleminen teknisellä laitteella tai tilanne kameravalvontaan on henkilön oma lupa esimerkiksi työpaikalla (Sallinen ym, 51-52). Henkilöiden kuvaamista luvalla ei voida kuitenkaan toteuttaa tiloissa, jotka laki yksiselitteisesti määrittää salakatselun tunnusmerkistön täyttäviksi tiloiksi, kuten wc-tilat ynnä muut aikaisemmin luetellut.

Käsiteltäessä kameravalvontaa, voi myös rikoslain 24. luvun 8 § tulla kyseeseen tietyissä tilanteissa. Kameravalvonnassa tällainen yksityiselämää loukkaavan tiedon levittäminen voi tapahtua, mikäli esimerkiksi valvontakameroilla tallennettua, salakatselun merkistön täyttävää kuvamateriaalia välitetään jollakin julkisella tiedonvälitysmenetelmällä. Kuvan välittäminen voi nykyään tapahtua esimerkiksi sosiaalisten palveluiden kautta tai aivan reaaliaikaista kuvaa välittämällä. (Sallinen ym, 54.)

Koska tässä opinnäytetyössä tarkkaillaan kameravalvontaa terveysasemien, hammashoitolojen ja palvelutalojen kannalta, tulee salakatselussa huomioida myös rakennuksen erilaiset tilat. Kameravalvonnan kannalta nämä rakennukset voidaan jakaa yleisölle avoimiin sisätiloihin, hoituhuoneisiin sekä asukashuoneisiin, potilas- ja asukashuoneisiin, henkilökunnan pukutiloihin sekä asukkaiden yhteisiin tiloihin. Näistä tiloista ainoastaan yleisölle avoimissa sisätiloissa kameravalvonta on yksiselitteisesti sallittua. Palvelutalojen asukkaiden yhteisten tilojen kameravalvonnassa tulee huomioida, ettei valvonta tapahdu oikeudettomasti ja tarkkailtavan yksityisyyttä loukaten; lisäksi valvonnasta on ilmoitettava näkyvästi. Muissa edellä mainituissa terveysasemien, hoitolaitosten sekä palvelutalojen tiloissa kameravalvonta on kielletty. (Sallinen ym, 16.)

5 Kameratekniikka, etävalvonnan haasteet

Koska kameravalvonnan tekniikka ja siinä käytettyjen kameroiden tekniikka on muuttumassa, on kameravalvontajärjestelmää kehitettäessä syytä tarkastella myös uuden tekniikan tuomia mahdollisuuksia sekä mahdollisia haittapuolia. Viime vuosina merkittävin käynnissä oleva muutos on ollut tallennin- sekä kameratekniikan muuttuminen analogisesta kohti digitaalista. Perinteiset analogiset kasettitallentimet ovat korvautuneet digitaalisilla pc-pohjaisilla tallentimilla, jotka säilyttävät kameravalvonnan kuvan kovalevyllä. Itse tallentimiin kytkettävät

kamerat saattavat olla tekniikasta riippuen joko analogisia tai digitaalisia ja joihinkin tallentimisiin voi jopa kytkeä kummankinlaisia kameroita. Myös mahdollisuus kytkeä tallentimia lähiverkkoon tai Internetiin on tuonut uudenlaisia mahdollisuuksia etenkin etävalvonnan toteuttamiseen sekä järjestelmän etähallintaan. Osa kameroista on edelleen digitaalisten tallentimienkin aikana analogisia. (Nilsson 2010.) Kameravalvontajärjestelmää kehittäessä tulisikin pohtia, onko täysin digitaaliseen tekniikkaan siirtymisestä hyötyä kameravalvonnan kannalta, vai onko se vain yksi kuluerä lisää päivityksessä.

5.1 Analogitekniikan edut ja haitat

Nykyisissä kameravalvontajärjestelmissä analogisella tekniikalla tarkoitetaan lähinnä analogista kameratekniikkaa, kun taas itse tallentimet ovat hyvin pitkälti digitaalisia. (Sallinen ym, 22). Vanhemmassa analogisessa kameratekniikassa on omat hyvät ja huonot puolensa. Analogisen tekniikan huonona puolena voidaan pitää ensinnäkin sen vaatimaa kaapelointia: jokaiselle kameralle täytyy olla oma kaapeli kameralta tallentimelle. Tämä hankaloittaa puolestaan järjestelmän laajentamista, sillä lisättäessä uusia kameroita, täytyy jokaiselle vetää oma kaapelinsa videokuvalle sekä sähkölle. Toinen merkittävä huono puoli analogisessa tekniikassa on sen sallima rajallinen kuvan maksimiresoluutio. Kuvan suurin resoluutio eli tarkkuus on analogisessa järjestelmässä 720 x 576 kuvapistettä. Pienempi resoluutio tarkoittaa, että kuvasta pystytään erottamaan vähemmän yksityiskohtia kuin suuremmalla resoluutiolla. (Sallinen ym, 21-30.)

Analogisilla kameroilla on edelleen hyviäkin puolia, joiden vuoksi niitä on käytössä vielä nykyäänä. Analogiset kamerat ovat hankintahinnaltaan IP-kameroita halvempia sekä myös ylläpidoltaan digitaalisia kameroita halvempia. Analogisia kameroita käytettäessä tiedonsiirtokapasiteetti ei myöskään tule ongelmaksi, kuten IP-kameroita käytettäessä. Analoginen kamerajärjestelmä onkin digitaalista järjestelmää helpompi toteuttaa niin, että järjestelmä on luotettava. Mikäli kameravalvontajärjestelmässä joudutaan uusimaan kameroita, on analogisen järjestelmän etuna myös se, että kaikki kamerat ovat yhteensopivia eri järjestelmien kanssa. Ainoa kohta, jossa ongelmia yhteensopivuuden kanssa voi tulla analogijärjestelmässä, ovat kääntyvien kameroiden ohjausprotokollat. Analoginen kameravalvontajärjestelmä on myös toistaiseksi halvempi hankkia sekä ylläpitää kuin IP-kameroihin perustuva täysin digitaalinen järjestelmä. (Sallinen ym, 21-30.)

5.2 Digitaalitekniikan edut ja haitat

Digitaalisella tekniikalla tarkoitetaan tässä kappaleessa IP-kameroilla toteutettua kameravalvontajärjestelmää. IP-tekniikkaan perustuvalla kameravalvonnalla tarkoitetaan sellaista järjestelmää, jossa video, ääni ja mahdollinen muu tieto siirretään joko langallista tai langaton-

ta lähi- tai laajaverkkoa pitkin. Englanninkieliset lyhenteet ja termit näille kahdelle verkko-tyypille ovat Local Area Network (LAN) ja Wide Area Network (WAN). IP-kamerajärjestelmä muodostuu yleensä kameroista, itse verkon tarvitsemista yhdyslaitteista, tallentimesta sekä tietokoneesta, jossa on hallintaohjelmisto järjestelmään. Kameran ovat tietokonepohjaisia ja voivat sisältää monia lisäominaisuuksia, joita analogisissa järjestelmissä ei yleensä ole. Valvontaan käytetty tietotekniikka voi monesti olla aivan tavallista kaupasta saatavaa tietotekniikkaa, mikä helpottaa laitteiden hankkimista sekä tarvittaessa uusimista joko laitteistoa päivitettäessä tai hajonneita laitteita korvattaessa. (Technical guide to network video 2009, 7-8)

Digitaalisen järjestelmän haittoja ovat esimerkiksi se, että ulkopuolisen on mahdollista tunkeutua kameravalvontajärjestelmään joissain tapauksissa hyvinkin helposti. Tämä riski pätee etenkin silloin, kun kuvaa siirretään Internetin välityksellä. Joissain tapauksissa täysin ulkopuoliset henkilöt ovat tunkeutuneet kameravalvontajärjestelmiin, jotka siirtävät kamerakuvan langattomasti. Laitteita, joilla langattomiin kameravalvontajärjestelmiin voi tunkeutua, saa suhteellisen halvalla. Pahimmissa tapauksissa järjestelmään tunkeutuneet henkilöt ovat jopa lähettäneet kameravalvontakuvan sijasta jotain aivan muuta kuvaa valvontajärjestelmään. (Werth, 2008.) Ulkopuolisen on myös erittäin helppo tarkkailla täysin suojaamattoman digitaalisen kameravalvontajärjestelmän lähettämää kameravalvontakuvaa, mikäli sitä välitetään Internetin kautta. Käyttämällä esimerkiksi Googlen haussa tiettyjä hakusanoja on mahdollista päästä käsiksi useisiin tuhansiin suojaamattomiin valvontakamerakuviin. Pahimmillaan näissä suojaamattomissa järjestelmissä Internetin kautta yhdistänyt luvaton käyttäjä pystyy jopa hallitsemaan kameroiden suuntausta, muuttuvan polttovälin objektiivin suurennusta sekä mahdollisesti sytyttämään ja sammuttamaan kamerasalaoja. Internetistä järjestelmään tunkeutunut henkilö voi myös joissain tapauksissa asettaa järjestelmälle minkä tahansa salasanan, jolloin kameravalvonnan oikea käyttäjä ei enää pääse hallitsemaan omaa kameravalvontaansa. (Merrick, 2010.)

Digitaalisessa järjestelmässä joudutaan ottamaan huomioon se, että verkon kapasiteetti varmasti riittää. Kaistaa tarvitaan niin itse kameravalvontaan, kuin myös verkossa tapahtuvaan muuhun tiedonsiirtoon, joka saattaa olla yrityksen toiminnalta kameravalvontakuvaa huomattavasti tärkeämpää. Valvontakameroiden kaistanarvetta voidaan vähentää esimerkiksi pakkaamalla kuvaa enemmän, pienentämällä kuvan resoluutiota tai laskemalla kuvatahtia. Näiden keinojen käyttäminen liiallisesti voi kuitenkin johtaa siihen, ettei valvontakamerakuva ole enää yhtä hyödyllistä kuvanlaadun heiketessä liikaa. (Sallinen ym, 20-27.)

Kokonaan digitaalisen kameravalvontajärjestelmän huonona puolena voidaan pitää myös sitä, että järjestelmään tulee enemmän laitteita, joiden sähkönsaanti tulee pystyä varmentamaan. Kamerakuvaa ei voida välittää eteenpäin tai tallentaa, mikäli jokin verkon laitteista on pois

päältä sähkökatkoksen takia. (Kameravontajärjestelmät 2009, 157.) Etenkin isommissa lähiverkoissa on yleensä useampia kytkimiä sekä reitittimiä; näiden laitteiden jatkuva sähkönsaanti on verkon toiminnan kannalta oleellista, mikäli tiedonsiirron halutaan toimivan sähkökatkojen aikana. Mikäli esimerkiksi halutaan, ettei sähköjen katkeaminen aiheuta laajamittaisia katkoksia lähiverkon toiminnassa, tulisi muun muassa tärkeimpien reitittimien sähkönsaanti taata varavirtalaitteella (engl. Uninterruptible power supply) (Cisco 2010; Cisco 2003, 20). Toisaalta mikäli digitaalisessa kameravalvontajärjestelmässä käytetään Power over Ethernet -tekniikkaa, pystytään jopa kameroiden sähkönsyöttö varmentamaan esimerkiksi palvelinhuoneesta, jossa tallentimet sekä muut verkon laitteet sijaitsevat. Power over Ethernet -tekniikassa laitteille syötetään virta samaa kaapelia pitkin, jonka kautta ne siirtävät tiedon. (Technical Guide to Network Video 2009, 73.)

Digitaalisista kameroista etenkin korkeampaan tarkkuuteen pystyvillä megapikselikameroilla, on mahdollista saavuttaa huomattavasti analogista valvontakameraa korkeampi kuvan resoluutio. Megapikselikameroiden ongelmana on kuitenkin se, että ne toimivat tavallisia kameroita huonommin hämärissä ja pimeissä oloissa. Yleensä myös ulko-oloissa, etenkin nopeassa liikkeessä ja erilaisissa sääoloissa analogiset kamerat ovat vielä digitaalisia parempia. Mikäli kameran oma herkkyys ei riitä hämärässä valaistuksessa kuvan kaappaamiseen, voidaan pimeässä käyttää valon lisäämiseen joko tavallista valoa, tai vaihtoehtoisesti ihmissilmälle näkymätöntä infrapunavaloa. (Sallinen ym, 29-30, 33.)

Koska IP-kamerajärjestelmässä kaikki tieto siirretään lähiverkon kautta, ei kameroille tarvitse välttämättä vetää yhtä paljon kaapeleita kuin analogisessa järjestelmässä, jossa jokainen kamera tarvitsee oman kaapelinsa jo pelkälle videolle. IP-kamerajärjestelmässä voidaan käyttää jo olemassa olevia lähiverkkokaapelointeja, mikäli järjestelmän laajentaminen tulee ajankohtaiseksi jossain tilanteessa. Käytettäessä Power over Ethernet -tekniikkaa (PoE), kameralle tarvitsee vetää pelkästään lähiverkon kaapeli. PoE-tekniikassa kamera saa tarvitsemansa virran samaa lähiverkkokaapelia pitkin, jonka kautta se siirtää myös videon sekä muun mahdollisen tiedon. (Sallinen ym, 24-25, 28.) Power over Ethernet tekniikan käyttäminen auttaa osaltaan IP-kamerajärjestelmän sähkönsyötön varmistamisessa. Käytettäessä PoE-tekniikkaa voidaan kameroille sähkönsyöttävä laite varmistaa sähkönsyötöltään, jolloin kaikki kamerat saavat edelleen virtaa sähkökatkoksen tapahtuessa. Näin IP-kameravalvontajärjestelmän luotettavuutta saadaan parannettua jonkin verran ja sähkönsyötön varmentamiseen tarvittavien laitteiden määrää vähennettyä. (Technical guide to network video 2009, 73.)

IP-kameroiden etuna on myös mahdollisuus erilaisiin älytoimintoihin jo itse kamerassa. Kun osa toiminnoista on kamerassa, voidaan tallentimelle tulevaa kuormitusta vähentää etenkin isommissa järjestelmissä. Liiketunnistus on yksi asia, jonka IP-kamerat pystyvät tekemään

tarvittaessa säästämällä tallentimen resursseja. Digitaalisessa järjestelmässä pystytään helposti toteuttamaan tallentaminen niin, että kuvaa tallennetaan ainoastaan, kun kuva-alueella on liikettä. Mikäli tällaista tallennustapaa käytetään, tulee kuitenkin ottaa huomioon, että liikkeen tunnistus on säädetty riittävän herkästi ja että se varmasti tunnistaa liikkeen myös erilaisissa oloissa kuten hämärässä. Liiketunnistus on toki mahdollista myös analogisessa järjestelmässä, mutta silloin kameroita ei voida käyttää prosessissa apuna, vaan kaikki liiketunnistus tapahtuu itse tallentimessa. (Sallinen ym, 22-24, 32-33.)

Kameroiden kuvatahdin määrittämisen mahdollisuus on myös yksi IP-kameratekniikan eduista. Kuvatahdilla tarkoitetaan sitä, kuinka monta kuvaa sekunnissa kamera kaappaa. Tavallisissa analogisissa kameroissa kameroiden kuvatahti on aina 25 kuvaa sekunnissa. Digitaalisessa järjestelmässä käyttäjä voi kameras tekniset rajoitukset huomioiden säätää itse kameras kuvatahdin. (Sallinen ym, 20.) Kameran kuvatahti voi kuitenkin laskea kuvattaessa hämärässä, sillä kamera tarvitsee pidemmän ajan yksittäisen ruudun valottamiseen. Tällöin kameras käyttäjän on valittava, haluaako hän pimeässä valoisampaa videokuvaa hitaamman kuvatahdin kustannuksella vai päinvastoin nopeamman kuvatahdin ja hämärämmän kuvan. Korkeamman kuvatahdin käyttäminen digitaalisessa järjestelmässä tarkoittaa myös suurempaa kaistan sekä tallennuskapasiteetin tarvetta. (Technical guide to network video, 32, 107.) Kuten aikaisemmin on mainittu, hämärässä voidaan kuvan valaisemiseen tarvittaessa käyttää joko tavallista tai infrapunavaloa. Lisävalolla kuvatahtia pystytään hämärässä kasvattamaan ja samalla kyetään näkemään yksityiskohtia, jotka muutoin jäisivät näkymättä kuvan tummuuden takia.

Täysin digitaalisen kameravalvontajärjestelmän hallitseminen voi olla väärin toteutettuna pahimmillaan hyvin haastavaa. Digitaalisessa järjestelmässä tulee ottaa huomioon, että verkon kaikki laitteet ovat selkeästi hallittavissa ja että niiden valvonta, käyttö ja ylläpito on toteutettu huolellisesti. Digitaalisessa järjestelmässä myös erilaisten laitteiden yhteensopivuus on kyettävä ottaman huomioon, kuten myös mahdolliset laitteistoihin sekä ohjelmistoihin tulevat päivitykset. (Kameravalvontajärjestelmät 2009, 157.) IP-kameroihin liittyviä standardeja on kuitenkin olemassa jonkin verran, kuten esimerkiksi ONVIF- ja EN-standardit sekä PSIA:n IP-laitteiden normit (Sallinen ym, 29). Esimerkiksi ONVIF-standardissa IP-kamerajärjestelmien eri laitteista pyritään tekemään sellaisia, että ne ovat varmasti yhteensopivia keskenään. Standardin tarkoituksena on antaa järjestelmien ostajalle enemmän vapautta hankkia sellaista laitteistoa kuin hän haluaa. Lisäksi ideana on taata se, että käyttäjä pystyy tulevaisuudessakin hankkimaan vanhojen järjestelmien kanssa yhteensopivia tuotteita, riippumatta siitä, kuinka markkinat kehittyvät. Onvif-standardin ideana on myös vähentää järjestelmän kuluja, kun hankinnassa voidaan vapaammin valita erilaisista yhteensopivista komponenteista. (Onvif 2011a, 2011b.) Toistaiseksi IP-kamerajärjestelmien huonona puolena onkin niiden kalliimpi hankintahinta (Sallinen ym, 30).

5.3 Hybriditekniikka

Hybriditekniikka tarkoittaa kameravalvonnassa sellaisella tekniikalla toteutettua kameravalvontajärjestelmää, jossa tallentimeen on kytkettynä sekä analogisia että IP-kameroita. Hybridijärjestelmän hyvänä puolena voidaan pitää sitä, että järjestelmää käytettäessä voidaan helposti käyttää hyväksi mahdollisia vanhoja analogisia kameroita. Toisaalta myös uusien IP-kameroiden käyttöönotto on hybriditekniikassa helppoa, sillä nekin voidaan kytkeä tallentimeen suoraan. Toisaalta myös digitaalisessa järjestelmässä voidaan käyttää tarvittaessa analogisia kameroita käyttämällä apuna videopalvelimia. Videopalvelin on laite, joka muuntaa kameran analogisen signaalin digitaalisen järjestelmän vaatimaan muotoon. Yhteen videopalvelimeen on yleensä mahdollista liittää 1-4 kameraa. (Sallinen ym, 24-26.) Koska hybridijärjestelmässä tietoa siirretään lähiverkkoa pitkin, voi sen kohdalla tulla esille samanlaisia tietoturvariskejä, kuin digitaalisessa järjestelmässä, mikäli verkko on toteutettu huonosti.

5.4 Muut tekninen kehitys

Kameravalvontatekniikka itsessäänkin on uudistumassa monella eri tavalla. Osa näistä uudistuksista on nykyisen tietotekniikan kehittymisen mahdollistamia. Kameratekniikan muuttuminen analogisesta digitaaliseen aiheuttaa muutoksia laitteistoissa, mutta myös muita teknisiä uudistuksia on viime vuosina kehitetty. Uusista teknologioista kasvojentunnistus on yksi keino, jolla kameravalvonnan hyödyllisyyttä on pyritty parantamaan. Kasvojentunnistuksella voidaan tunnistaa esimerkiksi tunnettuja rikollisia tai muutoin häiriötä aikaisemmin aiheuttaneita henkilöitä ja tarvittaessa puuttua heidän toimintaansa. Kasvojentunnistuksen ongelmana on kuitenkin etenkin alkuaikoina ollut se, että tunnistettavan henkilön tulee olla mahdollisimman suoraan kameran edessä, jotta tunnistaminen onnistuisi luotettavasti. (CCTV: Constant Cameras Track Violators 2003, 18, 20) Toisaalta kameravalvonnan liiketunnistusta on pyritty myös kehittämään niin, että sillä pystyttäisiin tunnistamaan kielletyillä tai vaarallisilla alueilla oleskelevia henkilöitä. Esimerkiksi Yhdysvalloissa on kehitetty järjestelmää, joka pystyy tunnistamaan junaradan tasoristeyksessä oleskelevat henkilöt, jotka ovat järjestelmään määritetyillä vaaravyöhykkeellä. Ensimmäisissä testeissä järjestelmä pystyi tunnistamaan tasoristeyksessä tai junaradalla liikkuvat henkilöt antamatta kuitenkaan vääriä hälytyksiä. (Shah, Javed & Shafique 2007, 37-38.)

Ulkomailla kameravalvontaa on alettu käyttää perinteisen tilavalvonnan lisäksi myös toisenlaisiin tehtäviin. Esimerkiksi Yhdysvalloissa, joissa kameravalvontaa käytetään yleisesti vankiloiden valvontaan, on valvontakameroita hyödynnetty myös rahan säästämiseen sekä tarpeettoman matkustamisen vähentämiseen. Vankiloissa vartijat pystyvät kameroiden avulla tarkkailemaan isompia alueita vähäisemmällä henkilömäärällä kuin muutoin. Muusta käytöstä esimerkkinä toimii tapaus, jossa tuomittu henkilö pystyi kameroiden avulla puolustamaan itse-

ään oikeuden istunnossa suoraan vankilasta. Tällä menettelyllä piirikunnan poliisilaitos säästi yli 2000 dollaria matkakuluissa sekä muissa kuluissa. (CCTV: Constant Cameras Track Violators 2003, 17.)

5.5 Tietoturva

Tallentimien tietoturvaan tulisi myös kiinnittää huomiota: mikäli tallentimet kytketään mihin tahansa verkkoon, kasvavat tietoturvariskit aina jonkin verran. Kameravalvontaan käytettävän verkon tulisi olla toteutettuna niin, ettei sieltä pääse mitenkään yhteyteen Internetiin tai Internetistä kyseiseen verkkoon. Nykyisellään esimerkiksi joissain tallentimissa ei ole ollenkaan haittaohjelmien- tai viruksientorjuntaa, sillä niistä ei ole yhteyttä. Koska monet tallentimet perustuvat normaaliin Windows XP-käyttöjärjestelmään, aiheutuu myös sen haavoittuvuuksista ongelmia. Suorittaessani työharjoittelua Espoon kaupungilla, havaitsin että eräässä tallentimessa, jossa lisäksi ei ole viruksientorjuntaa, on asennettuna Windows XP:n päivitykset ainoastaan Service Pack 2 asti, kun uusin Service Pack Windows XP:lle on SP3. Päivityksien puuttuessa on käyttöjärjestelmässä erittäin paljon paikkaamattomia tietoturva-aukkoja, joita mahdollinen tunkeutuja voisi käyttää edukseen. Jo pelkästään Service Pack 3 korjaa XP:stä useita tietoturvapuutteita (Microsoft, 2011).

Toisaalta pelkän SP3-päivityspaketin asentaminen ei nykyisin ole enää riittävää, sillä senkin julkaisemisen jälkeen on tullut useita tietoturvapäivityksiä. Windows XP -käyttöjärjestelmän riskialttiutta lisää entisestään se, että kyseisen käyttöjärjestelmän päivitykset loppuvat kokonaan huhtikuussa 2014 (Microsoft, 2012). Käyttöjärjestelmän päivityksien loputtua kasvaa sen turvattomuus verkkoon kytkettynä entisestään, sillä mitään mahdollisesti löydettyjä tietoturva-aukkoja ei enää paikata. Tämän seurauksena mahdolliset järjestelmään tunkeutujat voivat käyttää hyvin monenlaisia tietoturva-aukkoja hyväkseen ja luvaton pääsy järjestelmään helpottuu entisestään.

Tarkkaillessani tallentimeen suoritettavaa huoltotyötä työharjoitteluni aikana, havaitsin että tallentimessa oli tietoturvapäivityksien puutteen lisäksi myös kameravalvontaohjelmiston asetuksissa sellaisia asioita, jotka aiheuttavat tietoturvariskin. Kyseisessä tallentimessa järjestelmän pääkäyttäjän oletussalasana oli edelleen käytössä sekä muiden käyttäjien salasanat olivat heikkoja ja täten nopeasti murrettavissa. Pääkäyttäjän oletussalasanan pystyy monesti selvittämään hyvinkin nopeasti laitteen käyttöohjeesta, jotka ovat nykyisin saatavilla Internetissä.

5.6 Etävalvonnan haasteet

Yrittäessäni löytää tutkimustietoa etävalvonnan eduista ja haitoista havaitsin, ettei tällaista tietoa löytynyt käytännössä mistään julkisista lähteistä. Kaikki tutkimukset vaikuttaisivat keskittyvän pelkästään kameravalvonnan tehokkuuteen ylipäättänsä, ei niinkään erilaisen valvontatyypin tehokkuuteen. Tässä kappaleessa käsitellyt etävalvonnan haasteet perustuvat edellä mainitusta syystä yleisiin isommissa kameravalvontajärjestelmissä oleviin haasteisiin. Koska etävalvontaa suorittaessa syntyy helposti erittäin suuri kameravalvontajärjestelmä, voi sellaista rakentaessa kohdata samanlaisia haasteita kuin paikallisesti valvotussa isossa kameravalvontajärjestelmässä.

Aktiivinen kameravalvonta voidaan jaotella valvonnan tyypin mukaisesti proaktiiviseen tai reaktiiviseen kameravalvontaan. Proaktiivisessa kameravalvonnassa valvontaa suorittava henkilö pyrkii havaitsemaan monitoreista tapahtumia, jotka vaativat toimenpiteitä. Joissain tapauksissa valvontaa suorittava henkilö ei välttämättä käytä minkäänlaista logiikkaa tarkkailuun, vaan suorittaa sen intuition pohjalta tai täysin satunnaisesti. Reaktiivisessa kameravalvonnassa toiminta perustuu eri lähteistä tuleviin hälytyksiin. Tällaista kameravalvontaa suoritetaan monesti silloin kun valvottavissa kohteissa on kaikista eniten toimintaa. (Keval & Sasse 2008, 9.) Mikäli tarvetta aktiiviselle kameravalvonnalle ei ole, ei varsinaiselle valvomollekaan ole tarvetta, vaan voidaan järjestelmälle luoda vain jokin työpiste, josta kameroiden tallentamaa materiaalia voidaan tarvittaessa katsella sekä luovuttaa esimerkiksi viranomaisille. (Sallinen ym, 39.)

Yleisesti kameravalvonnassa on monenlaisia teknisiä haasteita, etenkin mikäli se suoritetaan olemassa olevan lähiverkon tai Internetin kautta. Ensinnäkin kameravalvonnan välittäminen verkon kautta aiheuttaa jatkuvan kuormituksen verkolle eikä sellaista vaihtelevaa ja välillä hiljenevää liikennettä kuin muu tavallinen verkkoliikenne. Mikäli tällaista jatkuvaa kuormitusta ei ole otettu huomioon verkkoa suunnitellessa, saattavat vähemmän tehokkaat verkkolaitteet ylikuormittua liikenteestä, jolloin sekä kameravalvonnan liikenne että muu liikenne hidastuu. Normaalisti välittäessä videota IP-verkkojen kautta, ladataan videota etukäteen ja näytetään vasta, kun videota on jo ladattu jonkin verran, jolloin kaistaa ei tarvita yhtä paljon. Kameravalvonnassa tätä tekniikkaa ei kuitenkaan voida hyödyntää, sillä kuva pitää saada näkyviin lähes välittömästi sen jälkeen kun kamera on sen kaapannut. (Harris & Harris 2009) Tämä verkkoliikenteen ja sen kuormittavuuden vaikutus on erittäin vahva etenkin etävalvonnan suorittavassa keskuksessa. Itse kohteissa sinällään ei synny kuin kohteen omien kameroiden liikennevirta, mutta keskitettyyn valvomoon puolestaan tulee kaikkien järjestelmien kokonaisliikenne, joka etenkin suurella kameramäärällä kasvaa vain entisestään.

Valvottaessa suurta määrää kameroita on yksittäisen verkon laitteen kuormituksen lisäksi huomioitava myös valvonnan aiheuttaman kaistan tarpeen vaikutus koko verkolle. Esimerkiksi kameran lähettäessä 704 x 576 resoluution (4 cif) videota H.264 pakkauksella 10 kuvaa sekunnissa, luo jo tämä yksittäinen kamera noin 0,64 Mbit/s verran tietoliikennettä. Vanhempaa pakkausmenetelmää käyttävät kamerat tuottavat monesti tätäkin enemmän liikennettä kuvanlaadun ollessa kuitenkin monesti huonompi. (Harris & Harris 2009.) Jos järjestelmässä olisi yhteensä esimerkiksi 300 kameraa, tulisi kokonaiseksi tietoliikenteen määräksi 195,2 Mbit/s. Tämä liikenteen määrä tarkoittaisi sitä, ettei hitaampi 100 Mbit/s -verkko enää riittäisi kapasiteetiltaan kyseisien kameroiden liikennemäärän siirtämiseen keskitettyyn valvomoon. Nopeampi 1000 Mbit/s verkko mahdollistaisi tällaisessa tilanteessa kaiken liikenteen siirtämisen (IEEE 2008, 3). Etenkin valvomon kannalta vähänkään isompi kameravalvontajärjestelmä vaatii hyvin isoa tiedonsiirtokapasiteettia etävalvonnan mahdollistamiseksi.

Tiedonsiirron lisäksi iso etävalvonnassa oleva kameravalvontajärjestelmä vaatii huomattavan määrän tallennuskapasiteettia. Mikäli oletetaan, että syntynyt kaistanmäärä yhtä kameraa on sama 0,64 Mbit/s kuin edellisessä kappaleessa, syntyy 200 kameran järjestelmässä päivässä 1300 gigatavua kuvamateriaalia. Mikäli kuvamateriaali haluttaisiin säilyttää 28 päivän ajan, tarvittaisiin tallennuskapasiteettia yhteensä lähes 40 teratavua. Jos tämä kaikki tallennuskapasiteetti sijoitetaan yhteen tilaan, tulee laitteisto kuluttamaan sähköä helposti n. 4 kilowattia, ja tilassa tulee myös olla hyvä ilmastointi riittävän jäähdytyksen takaamiseksi. Tallennuskapasiteetin tarvetta voidaan vähentää esimerkiksi säilyttämällä eri tärkeysjärjestyksen kameroiden materiaalia eripituisia aikoja. Joissain organisaatiossa sisäänkäyntien ja ulostulojen kamerakuva säilytetään pidempään ja muiden kameroiden kuva lyhyemmän aikaa. (Harris & Harris 2009.) Näiden teknologisten vaatimuksien takia kaiken tallennuskapasiteetin sijoittaminen yhteen kohteeseen ei välttämättä ole kannattavaa kaikissa tapauksissa. Keskitetyssä tallennusjärjestelmässä järjestelmään tehtävät huoltotyöt ovat toki siinä mielessä helpompia, että kaikki laitteet sijaitsevat yhdessä kohteessa, eikä eri kohteisiin tarvitse matkustaa korjaamaan laitteistoja. Toisaalta sellaisen järjestelmän, jossa koko tallennuskapasiteetti on keskitetty yhteen tilaan, voi heikkoutena olla se, että tulipalo, vesivahinko tai muu onnettomuus aiheuttaa tallennusjärjestelmän toiminnan pysähtymisen. Toimivuutta on kuitenkin mahdollista parantaa käyttämällä toteutuksessa kahdentamista (Valtiovarainministeriö 2010, 30).

Tallennuskapasiteetin lisäksi toinen itse tallenteisiin liittyvä tekijä on tallennetun kameravalvontamateriaalin hallinta. Kun kameroita on riittävän paljon, on erittäin oleellista, että kaiken tallennetun materiaalin luettelointi ja indeksointi on järjestetty riittävän hyvin. Mikäli tallennettua kamerakuvaa halutaan hakea uudelleen näkyviin myöhemmin, auttaa kunnollinen luokittelujärjestelmä huomattavasti työskentelyä. (Harris & Harris 2009.) Viime aikoina tietotekniikan kehittyminen on mahdollistanut jopa sen, että valvontajärjestelmät pystyvät entistä

paremmin analysoimaan kameroiden tallentamaa tietoa. Videota analysoivat ohjelmistot pysyvät erilaisien sääntöjen sekä liikemallien tunnistuksen perusteella analysoimaan ja jopa indeksoimaan videokuvan tapahtumia eri tilanteiden mukaan. Järjestelmät pystyvät parhaimmillaan esimerkiksi tunnistamaan, että kameran tallentama kohde on ihminen ja lajittelemaan tallentuneet ihmiset heidän ulkonäkönsä eri piirteiden, kuten koon ym. mukaan. (Ferenbok & Clement, 1; 8-9.)

Mikäli keskitetyssä valvomossa suoritetaan aktiivista kamera valvontaa, voi kameroiden määrästä tulla myös sinällään ongelma. Jos yksittäistä valvomossa työskentelevää henkilöä kohden on liian monta tarkkailtavaa kameraa, heikkenee valvonnan laatu. Valvottaessa suurta määrää kameroita liian vähällä määrällä henkilöitä, saattavat jotkin kamerat jäädä pitkäksi aikaa ilman aktiivista valvontaa. Suurta määrää kameroita valvottaessa havainnointi vaikeutuu etenkin, mikäli yksittäistä näyttöä kohden on suuri määrä kamerakuvia. Kamerakuvien määrän kasvattaminen yksittäisessä näytössä pienentää aina jokaisen kuvan kokoa jonkin verran. Mikäli kuvia on liian monta yhdellä ruudulla, voivat kameroiden kuvat mennä niin pieniksi, että havainnointi käy erittäin vaikeaksi. Kun kameroiden määrä yksittäistä työntekijää kohden kasvaa riittävän suureksi, ei järjestelmää voida enää käyttää kunnolla aktiiviseen valvontaan, vaan siitä pystytään enää lähinnä tarkkailemaan eri hälytyksien perusteella tiettyjä kamerakuvia. (Gill ym, 2005, 7.)

Koska keskitetystä valvomosta on mahdollista päästä käsiksi useiden kohteiden kameravalvontakuviin, tulisi järjestelmien olla ensinnäkin suojattuna riittävän vahvoilla salasanoilla. Salasanat eivät saisi olla jostain tietyistä sanoista tai niiden yhdistelmistä muodostuvia. Myöskään kirjainten muuntaminen joksikin muuksi merkiksi esimerkiksi a-kirjaimen muuttaminen numeroksi 4 ei auta salasanan turvallisuuteen juuri yhtään. Hyvässä salasanassa tulisi olla paljon isoja ja pieniä kirjaimia sekä numeroita sekaisin. Satunnaisia merkkejä sisältävissä salasanoissa tulisi kuitenkin huomioida, että käyttäjä kykenee muistamaan salasanat riittävän helposti. Vahvuuden lisäksi salasanoissa tulisi huomioida, että ne vanhenisivat tietyin väliajoin ja ettei samoja salasanoja pystyisi käyttämään uudestaan. Hyvästäkään salasanasta ei ole luonnollisesti hyötyä, mikäli käyttäjä paljastaa sen esimerkiksi kirjoittamalla sanan lapulle ja jättämällä sen näkyville. (Alexander, S. 2004, 31-32.)

Salasanojen lisäksi verkkoon kytketyssä järjestelmässä on erittäin oleellista, että erilaisien ohjelmistojen haavoittuvuudet pyritään paikkaamaan mahdollisimman nopeasti niiden havaitsemisesta. Tietokoneiden ohjelmistoissa voi olla ohjelmointivirheitä tai asetuksissa virheitä, jotka vaarantavat tietokoneen tietoturvan. Tällaisiin tilanteisiin tulisi varautua tarkkailemalla haavoittuvuuksia erilaisista lähteistä ja esimerkiksi käyttämällä automaattista haavoittuvuuskientarkistus-ohjelmaa. Haavoittuvuuksia tarkistaessa tulee kuitenkin huomioida, että kaikki

haavoittuvuudet eivät välttämättä päde kyseisessä järjestelmässä, vaikka ohjelmisto niin ilmoittaisikin. (Mell, Bergeron & Henning 2004, 2-7, 2-8, 3-8.)

Vaikka valvontaan käytetyt tietokoneet eivät olisi kytkettynä Internetiin tai muuhunkaan verkkoon, on silti olemassa mahdollista, että koneeseen pääsee haittaohjelmia, jotka voivat pahimmillaan kerätä tietoja järjestelmästä hyökkääjän tarpeisiin. Ilman verkkoyhteyttä haittaohjelmat voivat päätyä koneeseen USB-muistien kautta. USB-muistit ovat hyvin yleisiä nykyisin ja ne voivat täten aiheuttaa tietoturvariskin mikäli, niitä käytetään huolimattomasti. Minkäänlaisia löydettyjä USB-muisteja ei tulisi kytkeä organisaation tietokoneisiin, ennen kuin tietoturvasta vastaava henkilö tai osasto on tarkastanut ne. USB-muistien kautta leviäviä haittaohjelmia voidaan torjua myös pitämällä kaikkien koneiden tietoturvaohjelmistot ajan tasalla sekä poistamalla käytöstä muistien automaattinen avaaminen liitettäessä. (McDowell, 2011.)

5.7 Valvomo

Koska Espoon sosiaali- ja terveystoimessa kameroita valvotaan tällä hetkellä ainoastaan kohteiden omista monitoreista, joudutaan kameravalvontaa keskittäessä luomaan niille kokonaan uusi valvomotila. Koska kameroiden määrä on erittäin suuri, on valvomon luominen haastavampaa, sillä suuresta määrästä kamerakuvia pitää pystyä erottamaan oleelliset asiat. Valvomon vaatimuksia käsittelevät muun muassa Finanssialan keskusliiton Kameravalvonnan K-menetelmä sekä Euroopan vakuutus- ja jälleenvakuutusyhtiöiden keskusliiton dokumentti CEA 4036 (Kameravalvonnan K-menetelmä 2006, 28). Tässä kappaleessa on käsitelty muun muassa valvomon ergonomisia näkökulmia sekä yleisiä kameravalvontaan liittyviä seikkoja.

Valvomoa perustettaessa tulisi ensinnäkin ottaa huomioon, että käytettävä tila on sopiva käyttötarkoitukseensa. Tilaa valittaessa tulisi pyrkiä huomioimaan se, että huone on riittävän suuri, ettei siellä ole haitallisesti tiellä olevia pilareita ja että huone on sopivan muotoinen käyttötarkoitusta varten. Tilan koolla on merkitystä useammassakin mielessä. Ensinnäkin riittävän iso tila mahdollistaa valvontaan käytettävien ruutujen hyvän sijoittelun sekä mahdollistaa järjestelmään tehtävät huoltotyöt niin, ettei valvontaa tarvitse lopettaa, jotta laitteisiin päästäisiin käsiksi huollon aikana. Toisaalta riittävän suuri huone mahdollistaa myös laitteiston määrän lisäämisen tulevaisuudessa, mikäli kameravalvontajärjestelmää laajennetaan. Jos laajennuksia on tiedossa, tulisi vapaata tilaa jättää niitä varten valmiiksi. Liian ahdas huone on myös työntekijöiden ergonomian kannalta huono. Valvomoa suunnitellessa on huomioitava myös se, että suurimmat laitteet saadaan mahtumaan huoneen ovesta sisään. Valvomon tulisi olla suhteellisen lähellä käymälätiloja, etenkin mikäli kameroita valvoo vain yksi henkilö. (Wallace, E. & Diffley, C. 1998, 3.)

Valvomohuonetta suunnitellessa tulisi ottaa huomioon työoloihin vaikuttavat ympäristötekijät. Suunniteltaessa valaistusta tulisi huomioida, että huoneessa tulee pystyä sekä tarkkailemaan valvontakameroiden kuvaa että lukemaan ja kirjoittamaan paperilla olevaa tekstiä. Mikäli valaistus on esimerkiksi kamerakuvan näkyvyyden parantamiseksi hyvin himmeä, voi kameroita tarkkaileva henkilö lukea paperilla olevan ohjeen helpommin väärin. Jos huoneeseen tulee ikkunoista luonnonvaloa, tulee niissä olla kaihtimet, joilla sisään tulevan valon määrää voidaan tarvittaessa säätää. Valvomon monitorit tulisi sijoittaa niin, ettei auringonvalo aiheuta niihin näkyvyyttä haittaavia heijastuksia, eikä aurinko paista suoraan työntekijän silmiin. Jotta valvomossa pystytään työskentelemään tarvittaessa pitkiäkin aikoja, tulee tilan ilmanvaihdoista sekä lämpötilansäädöstä huolehtia. Eri henkilöillä voi olla erilaisia mieltymyksiä sopivaan huonelämpöön, joten lämpötila olisi hyvä olla säädettävissä. Kameravalvonnan seurantaan tarkoitetut monitorit ja tietokoneet tuottavat hukkalämpöä, jonka vaikutus huonelämpötilaan on muistettava huomioida. (Wallace & Diffley 1998, 3-5.)

Valvomon työpistettä perustettaessa on myös huomioitava erilaisia tekijöitä, jotka vaikuttavat työergonomiaan. Ensinnäkin työpisteessä tulisi olla riittävästi jalkatilaa, jotta valvomon työntekijä mahtuu tarvittaessa vaihtamaan asentoaan. Liian ahtaassa tilassa työskentely voi käydä pidemmän päälle rasittavaksi ja heikentää keskittymistä itse valvomistyöhön. Valvomossa tulisi myös olla riittävästi pöytätilaa, jotta valvontaa suorittava henkilö pystyy tarvittaessa kirjoittamaan tietoja paperille sekä työskentelemään muutoin. Toisaalta pöydän tulisi myös antaa riittävä tuki työntekijän käsille, jottei hän rasittuisi pidempään työskennellessään. Huomioitavaa on myös se, että kaikki laitteet mahtuvat helposti työskentelytasolle niin, että niihin yltää helposti ja laitteistoja mahdutaan tarvittaessa huoltamaan valvomotyön keskeytymättä. Myös valvomon sisältämien laitteiden kaapeloinnit tulisi sijoittaa niin, etteivät ne ole tiellä aiheuttaen kaatumisia. (Wallace & Diffley 1998, 4.) Toisaalta pöytätilaa tulee olla myös riittävästi, jotta valvontaan käytettävien tietokoneiden näppäimistöille sekä hiirille olisi tarpeeksi tilaa niiden helppoa käyttämistä varten (Donald 2007).

Valvomotyön kannalta oleellinen on pöydän lisäksi myös tuoli, jossa valvomossa työskentelevä henkilö työnsä tekee. Siinä tulisi olla riittävän hyvät säädöt vähintään istuimen korkeudelle sekä selkänöjan kallistukselle ja korkeudelle. Säädöillä eri henkilöt saavat tuolin sopivaksi eivätkä saa tarpeettomia selkä- tai niskakipuja. Selkänöjan säädöllä on tarkoitus saada selkänöja tukemaan istujan selkää koko matkalta. Myös tuolin käsinojista voi olla hyötyä joko käsien tuen jatkona tai tuolista ylös noustessa. (Wallace & Diffley 1998, 5.)

Valvomossa työskentelevän henkilön suorituskykyyn vaikuttaa huoneessa olevien näyttöjen määrä, asettelu ja näytöissä näkyvien kamerakuvien määrä. Näytön koko tulisi pyrkiä suhteuttamaan siihen, kuinka paljon yksityiskohtia kuvasta pitää pystyä erottamaan sekä siihen, kuinka monta kamerakuvaa näytössä tulee näkymään. Liian pienestä näytöstä on vaikea nähdä

yksityiskohtia muualta kuin hyvin läheltä, mikä johtaa helpommin työntekijän rasittumiseen, kun hän joutuu keskittymään kuvan näkemiseen selvästi. Näytöt tulisi myös sijoittaa niin, että työntekijä pystyy istumaan hyvässä asennossa näyttöjä tarkkaillessaan ja näytöt tulisi mielellään olla säädettävissä niin, että eri henkilöt pystyvät säätämään ne itselleen sopiviksi. Näytöt, joita käytetään tarpeen vaatiessa kamerakuvan lähempään tarkasteluun, tulisi mielellään sijoittaa suoraan valvomotyöntekijän eteen tai vaihtoehtoisesti niin, että näyttöjä kohden voi kääntyä helposti. Lähempään tarkkailuun tarkoitettun näytön ympärillä olisi hyvä olla myös muita näyttöjä, joista näkee tarvittaessa yleiskuvaa tai muita tärkeitä kohteita. (Wallace & Diffley 1998, 6.)

Viimeaikoina myös isompien ruutujen, kuten esimerkiksi 42 tuuman näyttöjen käyttäminen kameravalvonnassa on alkanut yleistyä. Näiden isojen näyttöjen etuna on se, että niissä erilaiset kameroiden järjestelyt sekä käyttöliittymän järjestys voidaan muokata monipuolisemmin kuin pienempiä näyttöjä käyttäessä. Kuitenkin isojakin näyttöjä käyttäessä on huomioitava se, ettei niitä käytetä valvonnassa ainoastaan sen takia, että ruudulle saataisiin kerralla mahdollisimman paljon kamerakuvia. Kameravalvontaa tarkkaileva henkilö ei voi seurata vain rajallista määrää kamerakuvia niin, että hän pystyy edelleen havaitsemaan niistä oleellisia asioita. (Donald, 2007.)

Näyttöjen sijoittelun lisäksi oleellista on myös itse kamerakuvien looginen sijoittelu valvontaruuduilla. Mikäli tarkkaillaan useaa eri kohdetta, voidaan kamerakuvat järjestää esimerkiksi kohteittain, jolloin valvoja näkee helpommin, mikä kamera kuuluu mihinkin kohteeseen. Vaihtoehtoisesti kamerakuvat voidaan järjestää esimerkiksi sen mukaan, missä kohteissa tapahtuu kaikista eniten ja mitä täten joutuu tarkkailemaan eniten. Joka tapauksessa kamerakuvien tulee kuitenkin olla jossakin loogisessa järjestyksessä, jotta valvomossa työskentelevän henkilön on helpompi tarkkailla niitä loogisesti eikä vain satunnaisesti vaihtaa kuvasta toiseen. Kamerakuvien määrä henkilöä kohden tulisi myös rajoittaa. Mitä enemmän valvottavana on sellaisia kamerakuvia, joissa on paljon liikettä, sitä vaikeammaksi käy havaita oleellisia asioita näistä. (Wallace & Diffley 1998, 6.) Mikäli valvottavia kamerakuvia on paljon, voidaan järjestelmässä käyttää apuna liikkeentunnistusta. Liikkeentunnistuksessa voidaan määrittää alueita, joissa liikettä tarkkaillaan ja alueita joista sitä ei tunnisteta. (Technical guide to network video 2009, 102.)

Etenkin kokemattomien työntekijöiden kannalta valvomossa kannattaisi olla jokin selkeä karttajärjestelmä, josta kaikkien valvontakameroiden fyysiset sijainnit kohteessa näkyvät. Mikäli kamerat on kartoitettu interaktiivisessa karttajärjestelmässä, kykenee kameroiden valvontaa suorittava henkilö tekemään nopeammin erilaisia kameroiden tarkkailuun liittyviä päätöksiä. Järjestelmän tulisi olla integroituna kameravalvontajärjestelmään niin, ettei valvontaa suorittavan henkilön tarvitsisi erikseen katsoa toisesta järjestelmästä tai paperilta, mikä kamera on kyseessä. (Keval & Sasse 2008, 14)

Kameravalvontamateriaalin käytettävyyden kannalta on oleellista, että kuvamateriaali on tarpeeksi laadukasta, jotta siitä voidaan tunnistaa kuvissa näkyvät kohteet. Digitaalisessa järjestelmässä kameroiden kuvatahdin tulisi Keval & Sasse mukaan olla normaalisti vähintään 8 kuvaa sekunnissa tai vaihtoehtoisesti vähintään 12 kuvaa sekunnissa, mikäli kamerassa näkyvä kohde sisältää paljon liikettä. Lisäksi kuvaa ei tulisi pakata liikaa, sillä sekin heikentää osaltaan kuvan käytettävyyttä tunnistamiseen. (Keval & Sasse 2008, 15, 18.) Henkilöiden tunnistavuuteen vaikuttaa lisäksi henkilön koko suhteessa ruudun kokoon ja Finanssialan Keskusliiton tekemä opas neuvookin, että yksilöintiin henkilön koon tulisi olla 120 % kuvaruudun korkeudesta ja tuntemiseen 50 % ruudun korkeudesta. (Kameravalvonnan K-menetelmä 2006, 5.)

Rakennettavaan valvomoon sekä sen ominaisuuksiin tulee vaikuttamaan myös se, millaiseen käyttöön valvomoa ollaan rakentamassa. Jos tarkoituksena on suorittaa jatkuvaa aktiivista kamerakuvien tarkkailua, on valvomo toteutettava eri lailla kuin jos sieltä vain tarvittaessa noudetaan videomateriaalia tilanteissa, joissa jotain ei-suotavaa on tapahtunut. Osaltaan tähän valintaan vaikuttaa myös se, minkälaiseen järjestelmään kaupungin budjetissa on varattu rahaa kun kehittäminen tulee ajankohtaiseksi.

6 Kehittämisehdotukset, jatkotutkimus, työn arviointi

Kehittäessä kameravalvontaa Espoon sosiaali- ja terveystoimessa ainoastaan yhdestä kohteesta suoritettavaksi tulisi suunnittelussa ottaa huomioon erilaisia tulevaisuuteen liittyviä tekijöitä. Järjestelmää tulisi kehittää niin, että mikäli siihen tehdään laajennuksia tai mikäli jo uudistettua järjestelmää halutaan vielä yhdistää johonkin toiseen järjestelmään, olisi laajennuksien ja yhteensulauttamisten toteuttaminen mahdollisimman helppoa. Yhteensopivuuden kannalta olisi hyvä esimerkiksi pyrkiä hankkimaan laitteistoja, jotka noudattavat kameravalvonnan erilaisia standardeja ja näin sopivat helpommin yhteen uusien laitteiden kanssa. Standardien avulla järjestelmän käyttökelpoisuus voidaan jatkaa mahdollisimman pitkälle tulevaisuuteen.

Valvontakameratekniikka monimutkaistaa nykyisellään jossain määrin kameravalvontajärjestelmien kehittämistä. Mikäli kameravalvontajärjestelmää aiotaan muuntaa täysin digitaaliseksi, olisi Power over Ethernet -tekniikan käyttäminen erittäin suotavaa, maksimaalisen luotettavuuden takaamiseksi. Power over Ethernet tulee toisaalta myös vähentämään kaapelien tarvetta mahdollisissa uusissa asennuksissa, kun kameralle tarvitsee vetää ainoastaan tietoliikenteeseen käytetty verkkokaapeli. Kokonaisuudessaan täysin digitaalinen järjestelmä olisi myös tulevaisuuden kannalta todennäköisesti kaikista pitkäikäisin sekä helpoiten päivitettävissä jatkossa. Oleellinen asia digitaalista järjestelmää tehtäessä on ottaa huomioon erilaiset laitteiden yhteensopivuuteen liittyvät standardit. Etuina kokonaan digitaalisella järjestelmäl-

lä ovat myös mahdollisuus huomattavasti analogista järjestelmää parempaan kuvanlaatuun, sekä älytoimintojen toteuttamisen mahdollisuus niin, että tallentimen kuormitus pienenee. Järjestelmän pitkäikäisyyden sekä laajennettavuuden kannalta suosittelisin digitaalisen järjestelmän toteuttamista, sikäli mikäli se suinkin on mahdollista.

Koska valvottavien kameroiden määrä tulee olemaan erittäin suuri, tulisi järjestelmien mahdollisten älytoimintojen hyödyntämistä pyrkiä selvittämään ennen kehittämistyötä. Tällaisia toimintoja on esimerkiksi liikkeentunnistus ja sen perusteella tapahtuva kamerakuvan välittäminen. Koska valvottavia kameroita tulee olemaan yhteensä 442, tulee olemaan haasteellista järjestää niiden valvominen niin, että valvontaa suorittava henkilö oikeasti pystyy havaitsemaan kamerakuvista oleellisia asioita. Osaltaan valvomotyön toteuttamista helpottaa myös kamerakuvien looginen asettelu, johon tulee myös kiinnittää huomiota.

Keskitetty valvomo, tulisi suunnitella käyttötarkoitukseensa mahdollisimman sopivaksi. Mikäli valvomossa tulee työskentelemään henkilöitä, joiden ensisijaisena työtehtävänä on valvomo-kameroiden seuraaminen, tulisi mielellään heidän mielipidettä kuulla valvomoa suunniteltaessa ja luodessa. Valvomotyössä pidempään olleet kokeneet työntekijät osaavat suunnittelussa todennäköisesti huomioida paremmin sellaisia tekijöitä, jotka muilta mahdollisesti jäisivät huomaamatta.

Tarkkaillessani eräässä kohteessa kiinteistön kameravalvontajärjestelmän tallentimen asetusten päivittämistä, huomasin tallentimen kellon olevan noin viisi minuuttia todellista kellonai-kaa edellä. Mikäli kaikkia kohteita aletaan valvoa etäältä, tulisi huolehtia siitä, että eri tal-
lentimien kellonajat ovat yhteneväisiä. Jos pyritään etsimään johonkin tiettyyn aikaan tapah-
tuneeseen asiaan liittyvää tallennetta, tulevat poikkeavat kellonajat hidastamaan ja jossain
määrin vaikeuttamaan oikean kohdan löytymistä. Pidemmän ajan kuluessa saattaa poikkeama
oikeasta kellonajasta kasvaa merkittäväksi. Yksi keino pitää valvontaan käytettävien koneiden
kellot oikeassa ajassa on synkronoida ne esimerkiksi lähiverkossa tai Internetissä olevalta ai-
kapalvelimelta. Verkon sisäinen aikapalvelin olisi toisaalta tietoturvan kannalta parempi, kos-
ka kameravalvontaan käytetyiltä koneilta ei ole tarpeellista päästä Internetiin.

6.1 Jatkotutkimuskohteet

Opinnäytetyötä tehdessä yhdeksi mahdolliseksi jatkotutkimuksen kannalta mielenkiintoiseksi asiaksi nousi uusien, kehitteillä olevien älytoimintojen hyödyllisyys. Tässä työssä ei kyseisiin toimintoihin tarkemmin perehdytty lyhyttä esittelyä lukuun ottamatta. Tämänlaisen ison jär-
jestelmän osalta olisi mielenkiintoista tietää, kuinka esimerkiksi automaattisesti luvattomalla
alueella oleskelusta hälyttävät järjestelmät hyödyttäisivät valvontaa. Älyjärjestelmien avulla
voisi olla helpompaa vartioida suuren kameramäärän tuottamaa kuvadataa.

Opinnäytetyössä ei myöskään syvällisesti käsitelty sitä asiaa, millaisia hyötyjä tai haittoja suuren kameravalvontajärjestelmän yhdistämisestä keskitetyn valvonnan alle olisi. Tällaisesta asiasta ei julkisissa lähteissä ollut löydettävissä lähteitä, mikä osaltaan vaikeutti kyseisen asian käsittelemistä. Tätä asiaa pystyisi selvittämään esimerkiksi haastatteleamalla suurista kameravalvontakokonaisuuksista vastaavia henkilöitä ja kysymällä heiltä mitä hyötyä hajanaisen järjestelmän yhdistämisestä suuren kokonaisuuden alle olisi.

Koska kameravalvontajärjestelmät ovat monesti tavalliseen tietotekniikkaan perustuvia, olisi myös tietoturvallisuuden kannalta mielenkiintoinen jatkotutkimuskohde se, kuinka tallentimien käyttöjärjestelmät sekä muut ohjelmistot vaikuttavat näiden tietoturvaan. Jo pelkästään tallentimissa käytetyn Windows XP:n päivityksien loppuminen aiheuttaa lisää tietoturvauhkia sellaisiin tallentimiin, jotka ovat kytkettynä minkäänlaiseen verkkoon.

Tietoturvallisuuden kannalta mielenkiintoinen asia selvitettäväksi olisi myös se, kuinka kameravalvontajärjestelmissä voidaan suojautua mahdollisiin kohdistettuihin hyökkäyksiin. Esi-merkkejä tällaisista kohdistetuista hyökkäyksiltä ovat Flame sekä Stuxnet- virukset. Suojautuminen juuri kyseistä organisaatiota vastaan kohdistetuilta hyökkäyksiltä voi vaatia hyvinkin erilaisia keinoja, kuin yleisesti esimerkiksi viruksia ja haittaohjelmia vastaan suojautuminen. Tässä opinnäytetyössä en voinut näitä tekijöitä käsitellä osittain aikataulullisistakin syistä.

6.2 Opinnäytetyön arviointi

Opinnäytetyön työstämisen kannalta ehdottomasti huono asia oli alkuperäisen aikataulun venyminen merkittävästi siitä, mitä alun perin oli suunniteltu. Hitaan aikataulun vuoksi teoriaosuuksien sekä johtopäätösten kirjoittamisen välillä kului aikaa reilusti yli puoli vuotta. Aikataulua olisi työn aikana tullut seurata tarkemmin sekä tarvittaessa päivittää työn edetessä. Myös aikatauluun itse asetettujen määräaikojen noudattamisen olisi tullut olla tarkempaa kuin käytännössä työn aikana oli. Kirjoittamiseen tulleen tauon hyvänä puolena oli toisaalta se, että pidemmän ajan jälkeen työtä pystyi helpommin näkemään eri näkökulmasta kuin aikaisemmin. Työn ongelmia sekä mahdollisia kehityssuuntia oli helpompi tarkastella, kun tekstiä ei ollut työstänyt pidempään aikaan.

Käytettyjen menetelmien osalta opinnäytetyön heikkona puolena on se, että se on rakenteeltaan liian teoriapainotteinen. Sinällään opinnäytetyössä onnistuin mielestäni löytämään hyvin erilaisia lähteitä liittyen aiheeseen, etenkin kun huomioidaan hyödyllisen tiedon löytämisen vaikeus englanninkielisestä aineistosta. Työtä tehdessä olisi kohdeorganisaation kanssa tullut tehdä enemmän yhteistyötä, jolloin sisältö olisi enemmän sen tarpeita vastaava. Espoon kaupungin näkökulmaa työn sisältöön ja sen tarpeisiin olisi kannattanut hakea esimerkiksi teke-

mällä haastatteluja kaupungin turvallisuusorganisaatiossa työskenteleville. Haastatteluilla olisi opinnäytetyöhön ollut mahdollista saada huomattavasti laajempaa tiedonkeräysmenetelmien käyttöä.

7 Yhteenveto

Opinnäytetyössä oli tarkoituksena luoda katsausta siihen, millaisia asioita näinkin suurta kameravalvontakokonaisuutta keskittäessä sekä kehittäessä tulee huomioida. Kokonaisuutena opinnäytetyöstä tulee ilmi se, että suurta kameravalvontajärjestelmää luotaessa on otettava huomioon hyvin monenlaisia eri tekijöitä. Jo aivan perusasioita, kuten kameroiden sijoittelua sekä näkyvää kuva-aluetta suunniteltaessa tulee huomioida kaikkien kameravalvontaa koskevien lakien määrittämät rajoitukset. Myös tekniikan kehitys, sekä se että monissa kohteissa on edelleen jäljellä vanhoja analogisia kameroita, aiheuttaa omalta osaltaan haastetta järjestelmän mahdolliselle laajentamiselle sekä yhtenäistämislle yhden keskitetyn valvomon alle.

Kameratekniikan digitalisoituminen sekä käytettyjen tavalliseen tietotekniikkaan perustuvien tallentimien käyttäminen voi pahimmillaan huonosti toteutettuna aiheuttaa hyvinkin suuria riskejä kameravalvontajärjestelmään. Keskitettyä, suuria videomääriä käsittelevää järjestelmää toteuttaessa, tulisikin tietoturva toteuttaa erittäin huolellisesti. Tämä tarkoittaa sitä, että käytettyjen laitteiden tietoturvallisuuteen liittyvät haavoittuvuudet sekä muut yleiset riskitekijät on huomioitu järjestelmää suunnitellessa. Varautumisen kannalta kenties haastavimpia tietoteknisen tietoturvallisuuden osalta ovat organisaatiota vastaan mahdollisesti suunnatut kohdistetut hyökkäykset. Kohdistettuja hyökkäyksiä vastaan varautumiseen en valitettavasti opinnäytetyössä ehtinyt paneutua ajan puutteen sekä kyseiseltä hyökkäystyypiltä suojautumisen haastavuuden vuoksi.

Opinnäytetyössä en antanut kovin täsmällisiä kommentteja siitä, millaisena kameravalvontajärjestelmä tulisi toteuttaa. Järjestelmän kehittämiseen tulee osaltaan vaikuttamaan hyvin vahvasti sekin, millainen budjetti kameravalvontaan on käytettävissä. Erilaisilla valinnoilla, kuten sillä, käytetäänkö analogisia vai digitaalisia kameroita, sekä valvotaanko kameroita aktiivisesti, voidaan vaikuttaa toteutuksen hintaan. Aktiivisen sekä passiivisen valvonnan edut ja haitat tulisi punnita tarkkaan, ennen kuin järjestelmää aletaan kehittää. Toisaalta uudistaessa järjestelmää, mikäli käytetään sellaisia laitteita, jotka ovat mahdollisimman pitkään käytökelpoisia, voidaan mahdollisesti tulevaisuuden kehityskustannuksia vähentää. Järjestelmää keskittäessä sekä edelleen kehittäessä tulisikin kaikki valinnat punnita erittäin tarkasti sekä kaikki turvallisuuteen ja tekniikkaan liittyvät asiat toteuttaa hyvin huolellisesti. Näin voidaan vähentää tarvetta siihen, että järjestelmää jouduttaisiin jatkossa kehittämään, koska sen alkupeäinen suunnittelu ja toteuttaminen on tehty huonosti.

Lähteet

Alexander, S. 2004. Password protection for modern operating systems. Viitattu 17.9.2011
<https://db.usenix.org/publications/login/2004-06/pdfs/alexander.pdf>

CCTV: Constant Cameras Track Violators. 2003. NIJ Journal Issue No. 249 / July 2003.

Cisco. 2003. How Cisco IT-LAN-SJ Achieved High Availability. Viitattu 27.7.2011.
http://www.cisco.com/global/EMEA/ciscoitnetwork/pdf/cisco_it_high_availability.pdf

Cisco. 2011. Networking Basics: What You Need To Know. Viitattu 28.7.2011.
http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/networking_basics/index.html

Donald, C. 2007. CCTV control room design considerations. Viitattu 25.7.2011
<http://www.securitysa.com/regular.aspx?pkRegularId=2916>

Espoon kaupunki. 2011a. Sosiaali- ja terveystoimi. Viitattu 12.7.2011.
<http://www.espoo.fi/default.asp?path=1;28;11866;11869;39339;22478>

Espoon kaupunki. 2011b. Viranhaltijaorganisaatio 1.1.2011. Viitattu 12.7.2011.
<http://www.espoo.fi/binary.asp?path=1;28;11866;11869;39339;95511;95512;107649&field=FileAttachment>

Ferenbok J, & Clement, A. Hidden Changes: from CCTV to "Smart" video surveillance.
http://propid.ischool.utoronto.ca/video_surveillance/downloads/HiddenChanges.pdf Viitattu 17.9.2011

Gill, M. & Spriggs, A. 2005. Assessing the impact of CCTV - Home Office Research Study 292. Home Office Research, Development and Statistics Directorate.

Gill, M., Spriggs, A., Allen, J., Hemming, M., Jessiman, P., Kara, D., Kilworth, J., Little, R & Swain, D. Control room operation: findings from control room observations. Home Office Online Report 14/05. 2005. Home Office.

Harris, V. & Harris, C. 2009. Information overload: CCTV, your networks, communities and crime. Viitattu 5.8.2011.
<http://igneous.scis.ecu.edu.au/proceedings/2009/secintel/Information%20overload%20CCTV%20your%20networks,%20communities%20and%20crime.pdf>

Henkilötietolaki 22.4.1999/523

Honovich, J. 2009. Is Public CCTV Effective? Viitattu 5.8.2011.
http://ipvideomarket.info/report/is_public_cctv_effective

Huuhtanen, H. 2009. Kameravalvonnan rikostorjunnalliset vaikutukset liikkeenjohdon ja rikollisten näkökulmasta. Opinnäytetyö. Espoo: Laurea-ammattikorkeakoulu.

IEEE Std 802.3-2008. 2008. New York: The Institute of Electrical and Electronic Engineers. Viitattu 17.11.2012. http://standards.ieee.org/getieee802/download/802.3-2008_section3.pdf

Kameravalvonnan K-menetelmä. 2006. Helsinki: Finanssialan Keskusliitto. Viitattu 26.7.2011
http://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Kameravalvonnan_suunnitteluohje_K-menetelma_2006.pdf

Kameravalvontajärjestelmät. 2009. ST-Käsikirja 13. Espoo: Sähkötieto.

Sallinen, P., Ellonen, V., Kauppi, V., Kinnunen, H., Käykö, P., Laitinen, J., Lehtikangas, M., Lehtinen, T., Lehtonen, R., Pänkäläinen, A., Pöysä, H., Starck, K. & Woitsch, P. Kameravalvontaopas. Espoo: Turva-alan yrittäjät ry.
http://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Kameravalvontaopas_2010.pdf

Keval, H. & Sasse, A. M. 2008. "Not the Usual Suspects": A study of Factors Reducing the Effectiveness of CCTV. Viitattu 9.8.2011.
http://sec.cs.ucl.ac.uk/fileadmin/sec/publications/Keval_Sasse_Not_the_Usual_Suspects_Security_Journal_2010.pdf

Laki yhteistoiminnasta yrityksissä 30.3.2007/334

Laki yksityisyyden suojasta työelämässä 13.8.2004/759

Laki yksityisistä turvallisuuspalveluista 12.4.2002/282

McDowell, M. 2011. Using Caution with USB Drives. US-CERT. Viitattu 17.9.2011.
<http://www.us-cert.gov/cas/tips/ST08-001.html>

Mell, P., Bergeron, T. & Henning, D. 2005. Creating a Patch and Vulnerability Management Program. National Institute of Standards and Technology

Merrick, D. 2010. Hacking CCTV Systems with Google. Viitattu 27.7.2011. <http://www.david-merrick.com/2010/07/18/hacking-cctv-systems-with-google/>

Microsoft. 2011. List of fixes that are included in Windows XP Service Pack 3. Viitattu 1.8.2012. <http://support.microsoft.com/kb/946480>

Microsoft. 2012. Windows lifecycle fact sheet. Viitattu 31.5.2012.
<http://windows.microsoft.com/en-us/windows/products/lifecycle>

Nilsson, F. 2010. The Evolution of Video Surveillance Systems. Auerbach Publications. Viitattu 28.7.2011. http://www.infosectoday.com/Articles/Video_Surveillance_Systems.htm

Onvif. 2011a. Benefits. Viitattu 12.7.2011. <http://www.onvif.org/About/Benefits.aspx>

Onvif. 2011b. Why Onvif? Viitattu 12.7.2011. <http://www.onvif.org/About/WhyONVIF.aspx>

Rikoslaki 19.12.1889/39

Shah, M., Javed, O. & Shafique, K. 2007. Automated Visual Surveillance in Realistic Scenarios. IEEE MultiMedia Volume 14: Issue: 1, 30-39.

Tietosuojavaltuutetun toimisto. 2011. Kameravalvonta. Viitattu 28.6.2011.
<http://www.tietosuojafi/28994.htm>

Technical guide to network video. 2009. Axis communications.
http://www.axis.com/files/brochure/bc_techguide_33334_en_0811_lo.pdf

Työturvallisuuslaki 23.8.2002/738

Valtiovarainministeriö. 2010. Sisäverkko-ohje - Vahti 3/2010. Valtiovarainministeriö.

Valtioneuvoston asetus yksityisistä turvallisuuspalveluista 19.6.2002/534

Wallace, E. & Diffley, C. 1998. CCTV: Making It Work - CCTV Control Room Ergonomics. PSDB Publication No 14/98. Hertfordshire: Home Office, Police Scientific Development Branch.

Werth, C. 2008. To Watch The Watchers. Newsweek 10.10.2008. Viitattu 27.7.2011.
<http://www.newsweek.com/2008/10/09/to-watch-the-watchers.html>