Security and the Smart City: A Systematic Review

Author name and affiliation:

1. Julian Laufs (corresponding author) [a] *julian.laufs@ucl.ac.uk*
2. Hervé Borrion [a] *h.borrion@ucl.ac.uk*
3. Ben Bradford [a] *ben.bradford@ucl.ac.uk*

[a] UCL Jill Dando Institute of Security and Crime Science
35 Tavistock Square
WC1H 9EZ
London
United Kingdom

Abstract

The implementation of smart technology in cities is often hailed as the solution to many urban challenges such as transportation, waste management, and environmental protection. Issues of security and crime prevention, however, are in many cases neglected. Moreover, when researchers do introduce new smart security technologies, they rarely discuss their implementation or question how new smart city security might affect traditional policing and urban planning processes. This systematic review explores the recent literature concerned with new 'smart city' security technologies and aims to investigate to what extent these new interventions correspond with traditional functions of security interventions. Through an extensive literature search we compiled a list of security interventions for smart cities and suggest several changes to the conceptual status quo in the field. Ultimately, we propose three clear categories to categorise security interventions in smart cities: Those interventions that use new sensors but traditional actuators, those that seek to make old systems smart, and those that introduce entirely new functions. These themes are then discussed in detail and the importance of each group of interventions for the overall field of urban security and governance is assessed.

Keywords: Systematic review, smart cities, safe city, security technologies, security functions

1. Introduction

Rapid urbanisation and progress in information and communication technologies (ICT) are two of the most important phenomena impacting urban security planning and governance today (Cocchia, 2014; Zhu, Li, & Feng, 2019). The latter, especially, has shaped the concept of smart cities, an increasingly popular idea in recent years (Albino, Berardi, & Dangelico, 2015; Naphade, Banavar, Harrison, Paraszczak, & Morris, 2011; Ralko & Kumar, 2016). The implementation of smart city technology is hailed as the solution to many urban challenges such as transportation, waste management, and environmental protection (Alawadhi et al., 2012; Ankitha, Nayana, Shravya, & Jain, 2017; Gohar, Muzammal, & Rahman, 2018; Lella, Mandla, & Zhu, 2017; Zhang, Wan, Yang, & Yang, 2017a; Zhang et al., 2017b). While these issues are the focus of a growing debate about smart city development, aspects of security and crime prevention are often neglected (Ralko & Kumar, 2016).

As a result, the implications of new smart city security systems for crime reduction, security, and urban governance are rarely discussed. This systematic review attempts to address this gap by exploring the last ten years' worth of literature on new security technologies that can be considered to fall under the smart city concept. It aims to investigate the extent to which these new interventions correspond with traditional functions of security interventions, and how they affect urban planning and governance. Through an extensive literature search and an analysis of 121 studies, this article compiles a list of security interventions for smart cities, discusses and contrasts their functions with those of more traditional interventions, before ultimately proposing several changes to the conceptual status quo in the field.

In the following, we provide background information on the role of security in urban planning and smart cities. We then outline the core methodological principles and search strategy used in this review before presenting and discussing the findings.

2. Background: Smart cities and urban security defined

More than half the world's population lives in cities, and this unprecedented level urbanisation is only set to increase in the future (Jalali, El-Khatib, & McGregor, 2015; Zhang et al., 2016). While this shift has improved the life of many, the explosion of urban populations has led to far-reaching problems in many cities around the globe (Zhang et al., 2017b). To meet these challenges, governments are increasingly turning to the use of information and communications technologies (ICTs) and are aiming (or at least claiming) to make cities 'smart'.

While the term 'smart city' is today widely used, there is no coherent and broadly accepted definition; in fact, Ramaprasad, Sánchez-Ortiz, and Syn (2017) , find 36 different definitions from disciplines as diverse as urban studies, computers and information technology, sociology, and public health. Because this paper focusses largely on the technological aspects of smart cities and implications for urban planning and security, it adopts the definition suggested by Elmaghraby & Losavio (2014) of a smart city as a city that uses "information and communication technologies to increase operational efficiency, independently shares information within the system, and improves overall effectiveness of services and the wellbeing of citizens". Ramaprasad et al. (2017) provide a holistic discussion on the term and discuss different definitional approaches.

The term 'smart city' has spread around the globe, affecting urban development programmes and government strategies (Berry, 2018). Many government initiatives seek to create a broad range of services, ranging from smart transport and smart energy to smart citizens and education (Hall et al., 2000). Such future cities are heralded for their efficient use of ICTs embedded within the fabric of urban environments that aim to improve and rationalise public services in the future (Berry, 2018). These futuristic scenarios, however, often fail to recognise safety and security as a focus (Hartama et al., 2017). This is critical, as it is not only one of the most basic tenets of urban planning and management but also of human wellbeing — after all, safety and security are on the second bottom layer of the Maslow pyramid (McLeod, 2007). As such, safety and security constitute factors that are integral parts of human well-being and as such also of any smart city design (Reddy, Suresh, Phaneendra, Shin, & Odelu, 2018a).

While some articles acknowledge that rapid urbanisation leads to challenges for traditional safety and security infrastructure in cities (Isafiade & Bagula, 2017) and that these are critical issues for contemporary integrated urban developments (Benkő & Germán, 2016), this is only rarely reflected in the literature. Most of the studies that explore the impact of emergent ICTs have done so through critiques of governmental programmes, drawing largely upon insights of large scale evaluative studies and, in many cases, avoiding the discussion of real technological developments (Berry, 2015).

Slowly, however, the realisation that crime and security problems are not isolated but often impact all other factors of city life, and as such should become a central issue in the creation of smart cities, has gained traction (Borrion et al., 2019). Thus, this paper follows the notion that proactively ensuring the security and safety of the public is a basic operation of smart cities (Bourmpos, Argyris, & Syvridis, 2014).

One approach that aims to reconcile issues of crime prevention with new smart city developments is the safe city concept (Hartama et al., 2017). While initially conceived as a framework for safety for natural disasters, it quickly came to cover all aspects of safety within the city. In particular, the concept seeks to reconcile urban growth with the need for security through a variety of technological functions and by optimising the allocation of law enforcement resources (Castelli, Sormani, Trujillo, & Popovič, 2017; Oatley, Crick, & Bolt, 2015).

Furthermore, a safe city describes integration of technology and the natural environment that "enhances the effectiveness and efficiency of the process of handling the threat of crime and terror, to enable the availability of a healthy environment for citizens, and access to health, rapid response to emergencies" (Hartama et al., 2017). Effectiveness and efficiency in smart cities, however, imply far more than only efficacy or financial concerns (i.e. whether the designated task has been completed and how much it costs). They also include issues of citizen satisfaction and whether the innovation has created a benefit to those subjected to the intervention and beyond. This is imperative, as citizens are in the end at the centre of any urban safety intervention and central to creating a safe environment (Cagliero et al., 2015). Thus, gauging the perceptions of citizens on urban security is a key point in Smart City management, as it will ensure that cities not only prevent or respond to safety risks and security threats but that they also remain an attractive place to live in (Cagliero et al., 2015).

Beyond these definitional issues, it is important to understand what a smart city practically entails and how it functions. It is difficult to conceive of a *general* architecture for smart cities because of the extremely diverse range of devices, technologies, and services that may be associated in such a system, and because of the high degree of interdependence between various components (Jalali et al., 2015). As such, there are many different models that discuss what components and infrastructures a smart city needs (Gaur, Scotney, Parr, & McClean, 2015). Most, if not all, of these smart city architectures contain, however, three basic layers: A sensor layer, a network or processing layer, and a service or actuator layer (Filipponi et al., 2010; Gaur et al., 2015; Jalali et al., 2015; Zhang et al., 2017b).

The sensor layer consists of the various (often heterogeneous) data collection units (i.e. sensors). These can be deployed to measure almost anything in the city landscape. Examples include environmental factors like brightness or sound, cameras, RFID tags to monitor entire objects, or even participatory sensing through social media (Jalali et al., 2015). Data from this sensor layer is then delivered to the respective actuators via the network layer. This second layer provides the communication infrastructure to transport the data but also aggregates data from different sensors (Filipponi et al., 2010). The last layer then contains actuators, i.e. those units that bring about a physical change in the environment or provide the required service (in our case fulfil a crime prevention function) (Gaur et al., 2015). Most relevant for our discussion of smart security interventions are the sensor and the actuator layer, which is why they will be highlighted in the following discussion.

This distinction between the different layers is also useful to understand the smart city as a complex system made up of various components on different levels, reaching from single sensors to software and servers that integrate them and ensure communication between them (Zhang et al., 2017b). Crime prevention interventions in the sense of this paper are thus specific technological solutions that seek to address a distinct (crime-related) problem and make up one or several components of a smart city infrastructure either on one or on multiple layers.

The extensive literature search upon which our arguments are based sought to give an overview of the variety of functions new security technologies might fulfil. Overall, it aims to augment but also challenge the current conceptualisation of emergent technologies as crime prevention measures for smart cities. By switching the focus to the 'functions' of these technologies (i.e., their direct/proximal effects on the environment), this paper seeks to bridge the gap between the bigger picture of safe cities and security on one hand and deeply technological solutions on the other.

***Table 1**: Examples of technological components on different layers of smart city infrastructure. A single intervention may combine different components from one or multiple layers.*

Sensor Layer	**Network Layer**	**Actuator Layer**
RFID sensor	Transmission technologies	Retractable barricade
CCTV camera	Processing/computing units	Police response
Facial recognition camera	Compression/analysis software	Streetlights
Microphones	…	Speakers
Motion detection		Adaptable signage
WIFI-access points		UAV swarm
Crowd-sourcing app		Alarm
Light sensor		…
…		

3. Literature search

3.1 Search terms

Two methods were followed to narrow down the search terms for this review. As the term ‘smart city’ is contested and not consistently used throughout the literature, this article used the results of Cocchia's (2014) study to supplement the search strategy. Cocchia found that there is no coherent definition of the word 'smart' and that its use (along with other related labels) is often arbitrary, while at the same time identifying several core terms that are frequently used interchangeably. In addition, scoping searches were carried out to find appropriate search terms related to security and crime prevention.

Wildcards were used to include variants of words with the same word stem (e.g. ‘offend*’ would identify terms such as offend, offender and offending). The terms ‘police’ and ‘policing’ were preferred over the wildcard ‘polic*’ which returned an abundance of results related to policy. Thus, two categories of search terms were used:

1. Terms related to ‘smart city’, including ‘future city’, ‘intelligent city’, ‘digital city’

AND

2. Terms related to crime prevention, including ‘crim*’, ‘secur*’, ‘offend*’, ‘police’, ‘policing’, ‘law enforcement’

3.2 Inclusion/exclusion criteria

The results were screened against the following pre-set inclusion and exclusion criteria:

- Only literature from the past ten years was included (2009 - 2018) to ensure that interventions were most relevant to today's smart city environments.
- Only literature that was available in English and German was included for practical reasons.
- Literature that was otherwise unobtainable or that was missing full-text or abstract was also excluded.
- To circumvent the pitfall of publication selection bias, grey literature was included in the review (following Mlinarić, Horvat, & Šupak Smolčić, 2017; Wilson, 2009) a review based on a

biased collection of studies is likely to produce biased conclusions (Rohstein & Hopewell, 2009). However, this does not mean that all studies, regardless of methodological quality, were included. Instead, only those that met methodological quality criteria were included in the review to ensure an unbiased collection of high-quality empirical work aimed at answering the research question.

After a first round of sifting with the above-mentioned criteria, the following hierarchically layered selection criteria were employed:

• Articles must have thematic relevance (e.g. articles that mentioned either of the search terms as part of an enumeration were not considered, e.g. '*smart city technology* encompasses advances in transport management, *crime prevention* and other city services'.)

• Outputs had to have a focus on technology (e.g. articles should introduce or evaluate new technologies). Because smart cities do to a large extent depend on the innovation of existing systems, works that suggested improvements to currently existing security interventions were also included.

• Outputs should be related to crime prevention or the improvement of public safety/security

• Outputs that focussed on new crime opportunities in smart cities rather than crime prevention were excluded. This included literature on cybercrime opportunities or cybersecurity in smart cities unless they also made reference to opportunities to prevent those crimes.

3.3 Search strategy for identification of studies

Searches were carried out on the following search engines:

- General databases: Scopus, Web of Science, Proquest, Zetoc
- Technology specific databases: IEEE Xplore, ACM Digital Library
- Grey Literature Databases: British Library EThOS; Open Grey did not return any results.

Backward and forward searches were carried out once relevant articles were identified. This, however, did not yield any additional results.

3.4 Filtering stages

The reference list and sifting process were managed using the EPPI Reviewer 4 software. After all duplicates and articles that did not meet the basic inclusion and exclusion criteria were removed, the title and abstract of the remaining papers were scanned against the layered selection criteria. For those studies that were included based on title and abstract, the full-text was reviewed against the same criteria again to ensure that only relevant studies would be included in the final analysis.

3.5 Inter-Rater Reliability (IRR)

To ensure good inter-rater reliability and to avert personal biases in the selection of the studies, the original coding results were verified by four other coders. Each of the coders was assigned a random sample of 100 studies. The sample size was selected to ensure that coders became familiar with the criteria (Belur, Tompson, Thornton, & Simon, 2018). When the results were compared, there was a 94 per cent agreement between the four coders. In the case of most disagreements, the 'correct' coding (or that which was the final agreed coding) was usually that which had been agreed on by a majority of coders. Disagreements that remained were discussed in the group and brought to a resolution by elaborating the overall aim of the review. The discussions highlighted a lack of clarity on some aspects of the inclusion and exclusion criteria, especially on issues of research design, methodology, and type of outcome measure, but also more fundamentally about how to screen studies that did not meet the inclusion criteria but might nevertheless be relevant.

Following the suggestion by Feng (2014) to improve accuracy, chance agreement was removed from the estimation of reliability by calculating the κ-statistic (see also Belur et al., 2018; Viera & Garrett, 2005). With a κ-statistic of 0.81 and above in three of the four cases, we achieved near perfect agreement between the coders (Landis & Koch, 1977). Only in one case, a κ-statistic of 0.72 was reported, which however, still indicated substantial agreement (Landis & Koch, 1977). Overall the inter-rater reliability tests showed a high agreement between coders and thus strengthened the validity of this review.

4. Synthesis approach

Though some authors such as Wilson (2009) suggest that the credibility of a systematic review depends more on the number of studies used than on the method of synthesis, we will still briefly introduce the approach taken for grouping and analysing the included studies.

While the aim of any synthesis is to generate new knowledge grounded in the information of the individual research studies, the right methodological path to this new knowledge is not set in stone and depends heavily on the individual review (Thomas, O'Mara-Eves, Harden, & Newman, 2017a). Since this review spans across a variety of academic disciplines and fields, a thematic synthesis approach was chosen as the modus of analysis as it is especially suitable for analysing multidisciplinary datasets (Thomas et al., 2017a).

To address the research aims, we identified common themes across the included studies and analysed them in detail. As a starting point for this process, we used conceptualisations of traditional security functions for both the sensor layer and the actuator layer (Borrion, Tripathi, Chen, & Moon, 2014; Ekblom & Hirschfield, 2014) but then employed an iterative and flexible approach (Gough, Oliver, & Thomas, 2017). This means that while the review builds on a foundation of open questions and some secure initial concepts, it is equally thematically grounded in the studies it contains (Thomas et al., 2017a).

The initial concepts used in this review should be seen as a starting point that introduces a common language to compare and contrast the identified intervention, rather than a rigid theoretical framework. Their sole purpose was to provide a common denominator (i.e. the clustering of security technologies by their function) for developing new themes from the included studies (Boyatzis, 1998).

5. Initial concepts

In the following, we lay out key functions of security interventions both as sensors (i.e. for threat detection) and actuators (i.e. for crime prevention). The functions on both the sensor and the actuator layer are critical to the implementation of effective and efficient security systems. Table 2 brings together two conceptualisations to form a new set of initial concepts. The table merges the functions contributing to threat detection as identified by Borrion et al. (2014) with the functions pertaining to crime prevention as identified by Ekblom & Hirschfield (Ekblom & Hirschfield, 2014). The network layer was left out because there are no distinct frameworks that specify different functions on this layer and because they are not uniquely pertaining to crime detection or prevention technologies.

***Table 2**: Security functions on different layers of smart city infrastructure*

Situation Awareness – Focus on Sensor Layer	Intervention – Focus on Actuator Layer(after Ekblom & Hirschfield, 2014)
Detect: e.g. determining the presence of certain anomalies, substances, individuals or behaviours (Hardmeier, Hofer, & Schwaninger, 2005)	**Defeat**: physically block access and movement or block/obscure the information that offenders want to collect
Authenticate: e.g. verifying that an individual is a member of staff or that they have the right to access (after Adey, 2002)	**Disable/Deny**: equipment helpful to offenders such as bugs or cameras
Identify: e.g. determining the name of a given chemical substance (Federici et al., 2005)	**Direct/Deflect**: offenders towards/away from place or behaviour
Locate: e.g. determining the location of individual passengers considered as potential threats to the infrastructure (Lee, Smeaton, O'Connor, & Murphy, 2005)	**Deter-known** offenders know what the risk of exposure is and judge it unacceptable so abandon/ abort attempt
Profile: e.g. classifying passengers who fit the profile of an offender for extra security checks (Sweet, 2008)	**Deter-unknown**: offenders uncertain what control methods they are up against, so again judge risk of exposure unacceptable
Track: e.g. following the movement of certain passengers through station premises (McCoy, Bullock, & Brennan, 2005)	**Discourage**: offenders perceive effort too great, reward too little, relative to risk, so abandon/abort attempt
	Demotivate: awakening, of offenders, emotions contrary to the mission, e.g. empathy with victims, removing excuses, coward image
	Deceive: offenders act on wrong information and are exposed to arrest or intelligence collection, frustrated, or mistakenly decide not to select this site as target
	Disconcert: causing offenders to make an overt involuntary movement or otherwise become startled

	Detect[1]: passive, and active exposure to make offenders self-expose by instrumental, expressive or involuntary action; by making legitimate presence/ behaviour distinctive; and by improving capacity of people exercising security role to detect **Detain**: once offenders are detected, they must be caught and held (or credible identifying details obtained so they can be traced) **Inform** (i.e. communicate): e.g. raising an alarm or calling in armed units in response to a detected threat (Kirschenbaum, Mariani, Van Gulijk, Rapaport, & Lubasz, 2012) **Manage**: e.g. performing resource allocation, tasking and scheduling (Olive, Laube, & Hofer, 2009)[2]

6. Results

After the first rounds of sifting, 209 documents were included for full-text analysis (figure 1). Out of these, 37 papers were not obtainable and a further 51 papers were excluded because their full-text did not meet the predefined criteria. This left 121 studies to be included in the final synthesis based on full-text screening.

[1] Note that the function to detect on the actuator layer is distinct from that on the sensor layer. Actuators with the function to detect can – similarly to the detain function – be seen as an enforcement action with the goal of removing the offender presence, whereas sensors merely seek to detect anomalies or illicit action.

[2] While this function may in some cases be considered to refer to the network layer of an intervention, we categorise it as an actuator. This is because managing the interplay of different interventions has a much more direct impact on security and crime prevention in a smart city context.

Figure 1*: Search stages and results of the systematic review*

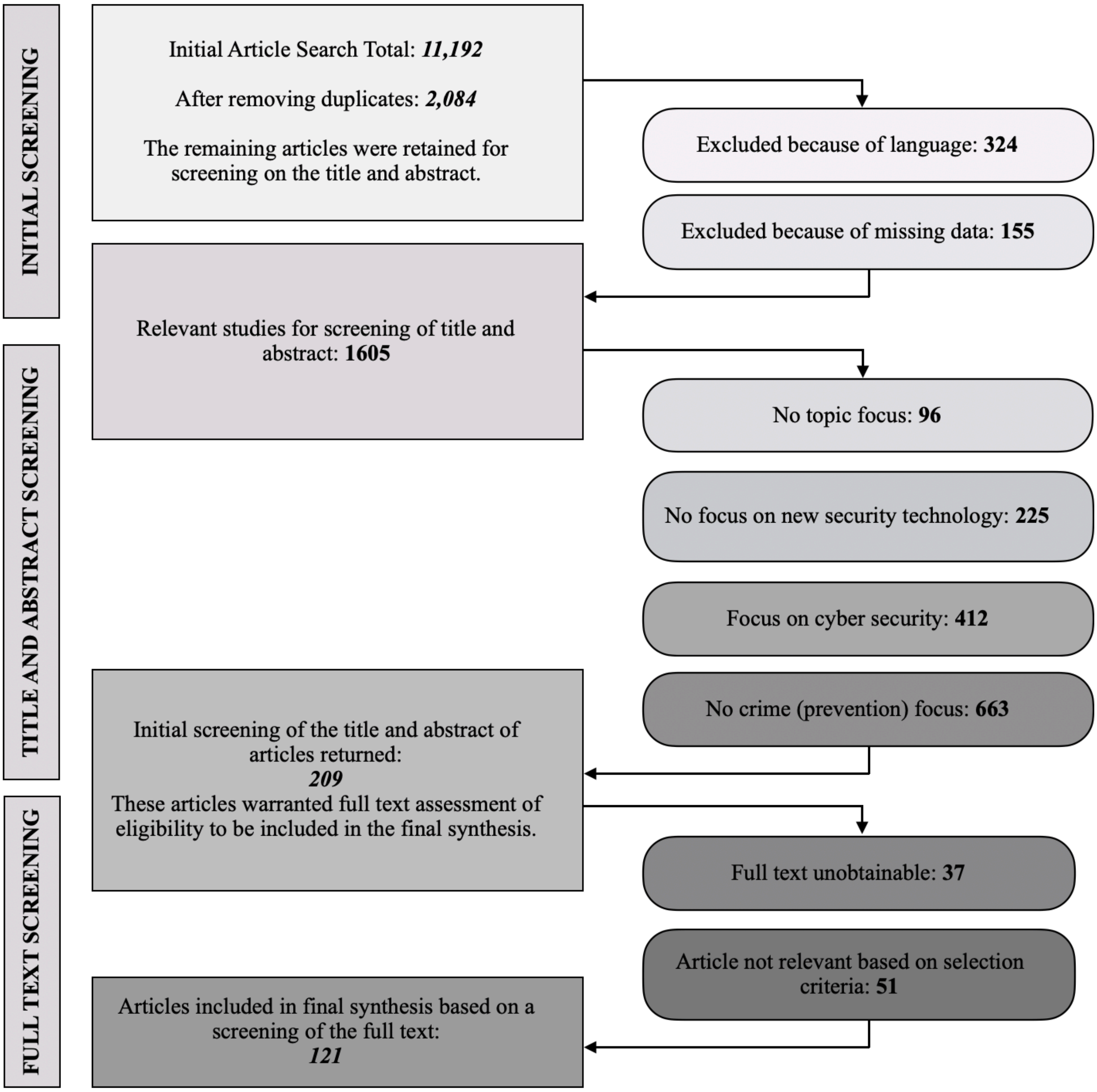

Table 3: *Results of the systematic literature search by category*

New sensors, traditional actuators	**43**
Detect and prevent unwanted or criminal behaviour	34
Identify, authenticate, defeat (potential) offenders	9
Making old systems smart	**57**
Improve/automate processes in order to adjust them to a smart city environment	32
Manage/Integrate the interplay of different existing security solutions	25
Entirely new functions:	**21**
(Mass) information and crowd-sourcing about criminal activity or public disorder	13
Predict potential threats	8

7. Analysis

Before detailing the content of the 121 included studies, it is worth making three general observations. Firstly, the search showed that the literature on new crime prevention technologies and smart cities is characterised by a disparity between highly technical studies on one hand and conceptual studies on the other. While the former group of articles often neglects the bigger picture, the latter focusses on conceptual aspects of large smart city systems, usually with no real technological foundations. Only a few studies attempt to bridge this gap. Moreover, many works that seek to predict the future use of a specific technology become quickly outdated due to the fast-pace developments in the field.

Secondly, as smart cities are highly complex environments, there are many instances where single interventions fulfil multiple functions. This can either be multiple sensing or actuator functions or include a mix of both. The latter is especially the case for personal security systems such as the portable safety device proposed by Mahajan, Reddy, & Rajput (2018). The device comes in the form of a bracelet or small wearable item that automatically detects a threat to its wearer or can be manually triggered to a range of defensive mechanisms. While some of these functions were explicitly mentioned such as the raising of an alarm (inform), others were left implicit, such as deterrence effects or the triggering of other actuators that the technological solution may or may not have. Furthermore, the review identified a wide variety of technologies that do not explicitly carry out security or crime prevention functions by themselves, but which build upon and seek to improve existing technologies such as CCTV. With, 57 included studies, this field makes up almost half of the identified interventions.

Thirdly, as already outlined in the background section of this paper, there is no clear definition of smart cities or even of smart technologies. The definitional vagueness surrounding some of the core concepts of this nexus is clearly reflected in the literature, often leading to less meaningful conclusions and the lack of a common basis for discussion.

Despite these shortcomings of the overall field, three clear themes emerged from the technological interventions examined in this review. The first theme concerns new security technologies that fulfil clear traditional security functions such as to detect and prevent, or to identify, authenticate, and defeat (7.1). The second theme includes studies that are focussed on the process of improving and automating 'traditional' security functions (as outlined above), and those that contribute to the management and integration of services to create the bigger picture of a smart city (7.2.). The last theme this review found is concerned with those interventions that fulfil new functions that as such did not really exist before, including disseminating mass information and predicting trends or events (7.3.). Though many of these things may have been technically possible before, they lacked technological solutions that made a wide-scale implementation possible and feasible. In the following, these three themes will be described in more detail with regards to their aim, shortcomings, and implications for urban security, planning, and governance as a whole.

7.1 New sensors, traditional actuators

7.1.1 *Detect and prevent*

The search identified 34 interventions (Table 4) that aim to detect anomalies, threats, or unwanted behaviour. While some studies analysed human behaviour, facial expressions, or lip-movement to identify threats in individual people (Anagnostopoulos, 2014; Byun, Nasridinov, & Park, 2014; Rothkrantz, 2017b; Sajjad et al., 2018), others sought to detect fraudulent behaviour through the analysis of big data and crowd movement patterns (Cemgil, Kurutmaz, Cezayirli, Bingol, & Sener, 2017; Gupta, Chakraborty, & Mondal, 2017; Liu, Ni, & Krishnan, 2014; Rocher, Taha, Parra, & Lloret, 2018; Sadgali, Sael, & Benabbou, 2018). Even though many of these interventions operated to a large extent the sensor layer of the smart city and relied on already existent actuators, they often did include secondary functions. This included automatically informing the police if fraudulent or dangerous behaviour was detected (Venkatesan, Jawahar, Varsha, & Roshne, 2017), and actuators aimed at de-escalating situations through environmental modification such as changes in light, sound, or smell (Al-Anbuky, 2014; Schuilenburg & Peeters, 2018). Secondary functions were also included in the four interventions with the aim to track the movement of persons, vehicles, or UAVs, which in case a threat was detected, could independently contain it (Anees & Kumar, 2017; Brust et al., 2017; Reddy, Loke, Jani, & Dabre, 2018b; Saravanakumar, Deepa, & Kumar, 2017) (Table 5).

Table 4: *Interventions with the primary function to detect.*

Author (Year)	(Crime) Problem	Solution	Primary security function	Secondary security function
Cho (2012)	Visual emergency detection	Detection and recognition method for emergency and non-emergency speech.	detect	
Liu et al. (2014)	(Charging) fraud in Taxis	Uses GPS speed and location data to compute the actual service distance on the city map, and detect fraudulent behaviours	detect	
Byun et al. (2014)	Offender identification and prediction	Detect crimes in real-time by analysing the human emotions	detect	
Bourmpos et al. (2014)	Prevention of crises (critical infrastructure)	Fibre sensing network to monitor diverse parameters of infrastructures, environmental conditions, and vehicle traffic	detect	
Giyenko and Im Cho (2016)	Faults of static CCTV	Intelligent IoT platform to facilitate the use of UAVs	detect	
Baba, Pescaru, Gui, and Jian (2016)	Stray dog attacks	Dangerous behaviour detection of group of stray dogs	detect	
Gupta et al. (2017)	Energy theft	Clustering based energy theft detection technique	detect	
Cemgil et al. (2017)	Fraud in meter readings	Fraud detection mechanism on the electricity consumption data	detect	

Welsh and Roy (2017)	Gunshot detection	Utilising 10 different sensors to detect gunshots	detect	
Bellini, Cenni, Nesi, and Paoli (2017)	Monitoring the flow of people	System to monitor the use of WiFi access points to determine how and where traffic is flowing	detect	
Baldoni et al. (2017)	Faults of static CCTV	Capillary video surveillance platform using plug-and-play that is flexible and scalable with the number of transmitting and receiving devices	detect	
Cubik et al. (2017)	Perimeter protection	Use of fibreoptic sensors in perimeter protection.	detect	
Ertugrul, Kocaman, and Sahingoz (2018)	Mapping and surveillance of buildings	Autonomous UAVs for indoor mapping of buildings and physical security control	detect	
Borges et al. (2017)	Detection of crime hot spots	Analyses characteristics of the urban environment to detect categories and hotspots of criminal activities	detect	
(Sajjad et al., 2018)	Facial expression recognition	Suspicious activity recognition based on facial expression analysis	detect	
Sadgali et al. (2018)	Credit card fraud	Detection of fraudulent transactions from big data using machine learning	detect	
Chackravarthy, Schmitt, and Yang (2018)	Backlog of video data created by traditional CCTV	Neural networks in combination with a Hybrid Deep Learning algorithm to analyse video stream data	detect	manage
Durga, Surya, and Daniel (2018)	Faults of static CCTV	Android application that obtains video feed, images and sound clips from the users and then uses cloud services for video enhancement and restoration of the content	detect	
Calavia, Baladrón, Aguiar, Carro, and Sánchez-Esguevillas (2012)	Faults of static CCTV	Intelligent video surveillance system able to detect and identify abnormal and alarming situations by analysing object movement	detect	authenticate
Datta and Sarkar (2017)	Faults of static CCTV	A flexible surveillance system using smart phones and existing sensors as well as home automation	detect	authenticate
Hu and Ni (2018)	Vehicle/object detection + license plate recognition	Automated object detection for urban surveillance systems	detect	authenticate
Manasa (2016)	Concealed explosives	Nanoscale technologies to find hidden explosives.	detect	identify
Agha, Ranjan, and Gan (2017)	Illegal racing/tail pipe modification	Automatic noisy vehicle surveillance camera	detect	identify
Rocher et al. (2018)	Fraudulent use of dyed fuels	IoT system to detect the presence of low-taxed fuels in the deposit of cars	detect	identify
Rothkrantz (2017a)	Sound recognition in CCTV	Lip-movements of a talking mouth can be recorded and understood, and aggressive behaviour detected	detect	improve
Venkatesan et al. (2017)	Theft	IoT based security system for homes, offices, banks. Sensors for theft and fire detection. Can automatically notify the user and automatically captures images of the intruder.	detect	inform

Ahir, Kapadia, Chauhan, and Sanghavi (2018)	Harassment, molestation	Smart device for women, including GPS/vital tracking, alarm, force sensor, and shock function	detect	inform
Eigenraam and Rothkrantz (2016)	Traffic rule violations/ suspicious behaviour	Multi-camera surveillance systems designed as a Decision Support System (DSS)	detect	locate
de Diego, San Román, Montero, Conde, and Cabello (2018)	Faults of static CCTV	Distributed intelligent video surveillance architecture based on Wireless Multimedia Sensor Networks	detect	track
García, Meana-Llorián, G-Bustelo, Lovelle, and Garcia-Fernandez (2017)	Faults of static CCTV	Analysis of pictures through Computer Vision to detect people in the analysed pictures	detect	manage
Anagnostopoulos (2014)	Suicide in metro stations	Information system architecture which can predict whether an individual intends to commit a suicide	detect	predict
Al-Anbuky (2014)	Street crime	Sensor-actuator smart public lighting network	detect	prevent
Schuilenburg and Peeters (2018)	Crime in night-time economy	Sound, smell and lighting programming combined with data analysis is used to reduce violence and aggression	detect	prevent
Huang and Chu (2017)	Trapped people	Detect trapped-victims underneath fallen objects	detect	track

***Table 5**: Interventions with the primary function to track as well as an integrated containment function.*

Author (Year)	**(Crime) Problem**	**Solution**	**Primary security function**	**Secondary security function**
Saravanakumar et al. (2017)	Vehicle theft, speeding	Track vehicles that commit crime and enable decision making at neighbouring traffic sites.	track	contain
Brust et al. (2017)	Malicious UAVs	UAV defence system for the purpose of intercepting and escorting a malicious UAV outside the flight zone.	track	contain
Reddy et al. (2018b)	Re-identification in CCTV	Facial recognition system to track or search a target person from a real time video feed	track	improve
Anees and Kumar (2017)	Crowd-density scanning	Key-point descriptors extracted from the scene are used to compute the dense areas which is further used to define the direction of the flow	track	manage

Technologies for the detection of threats through the collection and use of large amounts of data and technological measures to prevent crime long existed and are in widespread use today (e.g. CCTV). The automatic and local containment of unwanted behaviour or dangerous situations without the involvement of the broader security infrastructure (e.g. police services) or in some cases any human input is, however, new. Interventions that fall into this category often bring sensor and actuator layer closer together by creating a single intervention or by changing or adding new actuators to the equation. This does not only have an impact on crime prevention but also on urban planning and governance processes as a whole. Self-contained interventions pose fundamentally different requirements to urban planning and governance than those that require external actuators such as police interventions. An example of this are audio sensors that, if commotion is recognised, turn up the streetlights rather than triggering more traditional actuators like a police response (Al-Anbuky, 2014; de Kort et al., 2014). Because these interventions rely on the interplay of different smart city components to alert authorities, self-contained security interventions rely on the broad implementation of smart infrastructure across other realms such as lighting and the far-reaching deployment of more elaborate sensors and actuators (de Kort et al., 2014). This is also emblematic of the difficulties inherent in the retrofitting of existing cities with smart technologies brings about. Because smart interventions rely so heavily on each other and because a broad implementation across various realms opens up a variety of possibilities, it is inefficient to 'divide and conquer', i.e. to modernise sector after sector (Rathore, Ahmad, Paul, & Rho, 2016; Zygiaris, 2013). Since the usefulness of self-contained interventions is highly dependent on a holistic approach, it poses significant challenges to current processes of urban governance and especially modernisation efforts. Thus, interventions that are made up of not only sensor technology but also of actuators that automatically contain a threat can potentially have a great effect on urban security as a whole.

In addition to these more practical requirements, crowdsensing and big data analytics promise some degree of privacy for individuals, whereas facial or motion recognition technologies rely on singling out persons from the larger group (Balla & Jadhao, 2018; Braun, Fung, Iqbal, & Shah, 2018). As such, the studies examined show that interventions that rely on motion or facial expression recognition are especially controversial in terms of privacy, bringing many new ethical considerations and requirements into the planning process for urban security (Marx, 1998; Parra & Lopez, 2017). These considerations are not only important to ensure an inclusive and rigorous data-protection regime in smart surveillance environments, but they also have operational significance for the planning, implementation, and often functioning of these security measures (Patton, 2000).

7.1.2 Identify, authenticate, defeat

These initial findings tie in with the five included studies (Table 6) that aimed to authenticate individuals or vehicles attempting to access a restricted area (be it a private property or a congestion zone in a city). Operationally, this was done either through Near Field Communication (NFC) (Castella-Roca, Mut-Puigserver, Payeras-Capella, Viejo, & Angles-Tafalla, 2017) or through camera surveillance systems relying on automated license plate recognition (Balla & Jadhao, 2018; Boukerche, Siddiqui, & Mammeri, 2017; Hadjkacem, Ayedi, Abid, & Snoussi, 2017; Rothkrantz, 2017a). While the latter to some extent often constituted an improvement or automation of an existing system, the interventions were considered distinct because they are independent systems for access control that could also be implemented without any prior interventions in place. As such, the systems posed a significantly lesser challenge to urban security planning than those mentioned in the previous section.

Table 6: *Interventions with the primary function to authenticate.*

Author (Year)	(Crime) Problem	Solution	Primary security function	Secondary security function
Castella-Roca et al. (2017)	Vehicle access to restricted zones	Driver's smartphone is used to validate the access to a restricted zone	authenticate	
Balla and Jadhao (2018)	Unauthorised access	Intelligent security system using facial recognition	authenticate	
Sajjad et al. (2017)	Identification of suspects	Cloud assisted facial recognition framework	authenticate	identify
Rothkrantz (2017b)	CCTV does not operate in real time	Use of surveillance cameras to localise and recognise faces from suspect individuals	authenticate	improve
Boukerche et al. (2017)	Vehicle re-identification	Automated vehicle detection and classification system.	authenticate	profile

The effectiveness of these measures relies to a large extent on the use of physical barriers to 'defeat' intruders or the threat of repercussions if they are caught violating access rules (e.g. fines). Access control measures have, however, especially in a smart city far more use than the explicitly mentioned actuators might suggest. Holistic smart city architectures could for example not only prevent vehicles from entering a controlled zone but could also track movement patterns and impose automatic fines (Barba, Mateos, Soto, Mezher, & Igartua, 2012). This would alleviate the need for controlling access to congestion or environmental protection zones in city centres by the police and thus save resources in the long run. The implementation of such smart access control measures could additionally help the expansion of ‘greener’ transportation and as such would positively impact other realms of smart city development in the future (Barba et al., 2012).

In addition to these static access control measures, Sajjad et al. (2017) introduce a cloud-assisted face recognition framework. They propose the use of nano-devices for a concealed and secure face recognition system. Wearing a small-sized portable wireless camera and a small processing unit for face detection and recognition on officer’s uniforms would allow for the identification of anyone police interact with, without the need for manual identification. While this is only an example, it is symbolic for a move to supplement current static CCTV systems through mobile components. Whether this includes body worn cameras, cars, or drones, it has the potential to severely change the way we think about urban surveillance. This has some clear benefits such as the ability for cameras to follow crime and to surpass issues of re-identification between cameras if suspects are on the move (Zhang & Yu, 2018).

Nevertheless, these benefits come at a cost. While most of the systems proposed in the literature are often minimally intrusive and offer maximum amounts of privacy (Castella-Roca et al., 2017), the use of wearable facial recognition devices, as proposed by Sajjad et al. (2017) should be seen as problematic. Though the system may offer some use to the police, the potential downsides of its implementation are grave. It would for example mean that police officers could not be approached without citizens being subject to facial recognition, which in turn may dissuade many from approaching the police. This has important implications for citizens in their relations and contacts with police actors. This intervention in particular shows that privacy and data protection concerns are not only important on a legal level but also raise the question to what extent an intervention like this can have negative consequences for existing measures and in how far it can be reconciled with the citizen focus of the smart city concept (Braun et al., 2018).

7.1.3 Section summary

Overall, this study has identified a substantial body of literature concerned with using new sensors to detect criminal behaviour and identify individual perpetrators, often relying on already existing actuators for deterrence and crime prevention. Many of the identified interventions could transform urban security and the vision of a safe city. They reinforce the idea that in a smart city, many new security interventions rely on the broad implementation of smart technologies across different realms of the urban environment. Because security interventions no longer only rely on input from the police or their own sensors but can draw from a broad array of data sources, they become significantly more all-encompassing and holistic. Security measures no longer rely solely on the policy or a far-reaching security apparatus in a city but their effectiveness also relies on smart technologies in other realms such as street lighting or traffic management (Vitalij, Robnik, & Alexey, 2012). A lack of smartification in one realm can thus have impacts on the effectiveness of interventions in all other realms, first and foremost security interventions. This has great implications for the planning process of smart cities and their security infrastructure itself and shows that future security infrastructures are not separate systems but both reliant on and a prerequisite for the implementation of smart systems across other realms of city services.

This, however, does not mean that new interventions are uncontroversial. Privacy and data protection issues are at the forefront of concerns that may arise with their implementation and that need to be addressed in the planning and implementation of safe city concepts (Braun et al., 2018). As such, the interventions clustered in this theme offer great potential, but also require a thorough and far-reaching rethinking of the planning process itself because systems become significantly more interconnected and the effectiveness of single components dependent on the broader infrastructure (Mishra & Kumar, 2013).

7.2 Making old systems smart

7.2.1 Improve/automate

While many of the previously introduced measures sought to introduce entirely new systems, this is often neither necessary nor feasible. Instead, old systems that function well and are already in place can be improved and processes automated in order to adjust them to a smart city environment. This review identified 32 studies that address this issue (Table 7).

***Table** 7: Interventions with the primary function to improve or automate.*

Author (Year)	(Crime) Problem	Solution	Primary security function	Secondary security function
Sudha (2015)	Faults of static CCTV	Parallel architecture for smart video surveillance	improve	
Sormani et al. (2016)	No datasets for training algorithms	Generation of datasets for training reasoning algorithms for predicting the likelihood of terrorist actions against specific assets and locations in urban environment	improve	
Xiong et al. (2017)	Re-identification in CCTV	Multiple deep metric learning method empowered by the functionality of person similarity probability measurement	improve	
Shi, Ming, Fan, and Tian (2017)	Facial recognition	Recognition algorithm based on multi- scale completed local binary pattern	improve	
Zheng, Sheng, Zhang, Zhang, and Xiong (2015)	Re-identification in CCTV	Weight-based sparse coding approach for person re-identification	improve	
Salmerón-García et al. (2017)	Faults of static CCTV	Cloud-based surveillance system.	improve	
Thomas, Gupta, and Subramanian (2017b)	Faults of static CCTV	Video summarisation to reduce amounts of data recorded	improve	
Singh, Patil, and Omkar (2018)	Computational cost in multiple object tracking.	Parallel solution which effectively handles the challenges of time-dependencies among the various sections of the video file processed during multiple object tracking	improve	
Saba (2017)	Latency issues in CCTV	Device to capture and compress images and mounted with PIR sensor to detect movement	improve	
Tian, Wang, Zhou, and Peng (2018)	Faults of static CCTV	Block-level background modelling (BBM) algorithm to support long-term reference structure for efficient surveillance video coding	improve	
Hadjkacem et al. (2017)	Re-identification in CCTV	New approach based-on the analysis of all the video data extracted from camera-networks	improve	manage
Zhang, Chowdhery, Bahl, Jamieson, and Banerjee (2015)	Re-identification in CCTV	Real-time distributed wire-less surveillance system that leverages edge computing to support real-time tracking and surveillance	improve	manage

Tan and Chen (2014)	Faults of static CCTV	Approach for fast and parallel video processing	improve	manage
Zhou, Saha, and Rangarajan (2015)	Faults of static CCTV	Using existing public bus transit system to collect data from the cameras and physically transport it to the bus terminus, to be uploaded to the data centre	improve	manage
Oza and Gohil (2016)	Faults of static CCTV	Cloud based surveillance system for live video streaming	improve	manage
Xu, Mei, Liu, Hu, and Chen (2016)	Faults of static CCTV	Semantic based cloud environment to analyse and search surveillance video data	improve	manage
Valentín et al. (2017)	Faults of static CCTV	Architecture for automated video surveillance based on cloud computing	improve	manage
Wang, Pan, and Esposito (2017)	Faults of static CCTV	IoT based elastic surveillance system using edge computing to perform data processing	improve	manage
Zhang et al. (2017a)	Human action recognition	Background modelling method from surveillance video	improve	manage
Mehboob et al. (2017)	Faults of static CCTV	3D conversion from traffic video content to Google Maps using time-stamped glyph-based visualisation	improve	manage
Zingoni, Diani, and Corsini (2017)	Moving object recognition	Algorithm capable of successfully recognising and classifying moving objects	improve	manage
García, Valentín, Serrano, Palacios-Alonso, and Sucar (2017)	Faults of static CCTV	Visualisation techniques for both local and global visualisation	improve	manage
Ramírez, Barragán, García-Torales, and Larios (2016)	Transmission latency of data (CCTV)	Wireless sensor network (WSN) using low-power devices for the transceiver process to improve the data management using both, storage and transmission data	improve	manage
Ma et al. (2018)	CCTV placement	Use of traffic patterns to improve the placement of CCTV cameras	improve	manage
Pereira et al. (2018)	Faults of static CCTV	Low-cost smart surveillance platform designed to create a ubiquitous environment and to adapt to the client's needs	improve	manage
Memos, Psannis, Ishibashi, Kim, and Gupta (2018)	Faults of static CCTV	Algorithm to use less memory at the wireless sensor nodes	improve	manage
Peixoto et al. (2018)	Faults of static CCTV	Gap filling algorithms to data missing problem in a smart surveillance environment	improve	manage
Kumar, Datta, Singh, and Sangaiah (2018)	Faults of static CCTV	Intelligent decision computing based paradigm for crowd monitoring	improve	manage
Miraftabzadeh, Rad, Choo, and Jamshidi (2018)	Re-identification in CCTV	Algorithm to extract and administrate the crowd-sourced facial image features (e.g., social media platforms and multiple cameras in a dense crowd, such as a stadium or airport)	improve	manage
Zhang and Yu (2018)	Re-identification in CCTV	Deformable convolution module to the traditional baseline to enhance the transformation modelling capability without additional supervision	improve	manage
Al-Shami, Zekri, El-Zaart, and Zantout (2017)	Traffic rule violations	Parallelization processes that enables the online processing of images by an embedded system	improve	manage
Jun, Chang, Jeong, and Lee (2017)	Faults of static CCTV	Collaboration-based Local Search Algorithm (COLSA)	improve	manage

The key premise of these studies is that current surveillance systems need improvements to be useful in the future. The scalability and cost-effectiveness of current systems depends largely on these improvements as increased amounts of data and the need for faster processing, drive demand for innovation (Valentín et al., 2017). The most prominent example of this are many video surveillance platforms in use today, which are presented with severe problems of efficiency and scalability when the numbers of data flow senders and receivers increase (Baldoni et al., 2017).

In addition, the scalability of modern surveillance systems is often limited by the human factor, driving the demand for automation (human operators can watch ten cameras, but will not be able to monitor 10 000 deployed sensors). Many studies that sought to automate processes that currently require manual input, focus on human re-identification in multi-camera surveillance networks (Hadjkacem et al., 2017; Zhang et al., 2017b; Zheng et al., 2015) or even introduce a wholistic automated system architecture that do entirely without human operators (Valentín et al., 2017). The latter, in particular, is needed to realise the complex system that is a smart city because it does not tackle the issue on merely one layer but improves sensors, processing, and actuators alike. These developments are also problematic when examining current planning processes for security infrastructure. In many instances, there is a disparity between private developments and security agencies. And even where security and crime prevention are considered as factors, developments are often planned with already or soon-to-be outdated systems (Morton, Horne, Dalton, & Thompson, 2012; Sandborn, 2007).

Due to steadily improving camera and sensor technology and their large-scale deployment, data streams are exploding in urban surveillance. This impacts the scalability of current systems massively as they 'outgrow' the current infrastructure (Brayne, 2017). These issues of scalability of older systems are tackled by interventions on the processing layer of the smart city, aimed at making the transmission, storage, and processing of data cheaper, easier, and faster (Memos et al., 2018; Saba, 2017; Singh, Majumdar, & Rajan, 2017; Thomas et al., 2017b; Zhou et al., 2015). While in this case, the processing layer plays a significant role as the key variable limiting the growth and the flexibility of the systems, it is also sensors and actuators where innovation has a relevant impact on crime prevention in the future.

Future systems aim to analyse data in real-time using artificial intelligence (AI) to allow for a quicker response in case of danger (Reddy et al., 2018b; Zhang et al., 2015). Because in many cases not enough historical data exists to train AI, or because the data has gaps that could affect the machine learning, some studies introduce approaches to generate dummy data that can be used for training (Peixoto et al., 2018; Sormani et al., 2016). Such approaches are especially noteworthy because they do not only address shortcomings of current crime prevention technologies but rather provide practical solutions to aid the implementation of other interventions.

Similarly, studies such as those of Ma et al. (2018) and Jun et al. (2017) highlight the need for improving not only existing software and hardware but also the methods and procedures by which the deployment of technologies is determined.. Ma et al. (2018) discuss new metrics for the sensible deployment of surveillance cameras but the essence of their research is transferable to many other contexts; if the urban landscape changes significantly, parameters for the allocation of security technologies will also change. Unless this is considered along the way, the planning of urban security runs danger of missing crucial developments and ultimately failing in the future.

In terms of urban security as a whole and implications for its planning, interventions that seek to improve and automate current security measures fulfil one of the most important functions. This is because in practice, only in few cases smart cities are built from the ground up. Thus, when speaking about building smart cities, we often mean the retrofitting and improvement of existing systems with smart technologies (Habibzadeh, Soyata, Kantarci, Boukerche, & Kaptan, 2018). As such it is crucial that we approach the smartification of cities holistically but at the same time maintain an eye for existing infrastructures as the basis for these developments.

7.2.2. Manage/integrate

A truly safe (smart) city is defined by increased integration of different systems and the boundary-less coordination of measures across all fields. This review identified 25 interventions that sought to integrate or to manage the interplay of different existing security solutions in urban environments (Table 8). The scope and focus of these interventions differed greatly, reaching from single-layer solutions tackling the complex interplay of different sensors (Camboim, Neto, Rodrigues, & Zhao, 2017; Chen, Xu, & Guo, 2013) to holistic integrated framework architectures that work to connect sensors and actuators across the city (Bartoli, Fantacci, Gei, Marabissi, & Micciullo, 2015; Dbouk, Mcheick, & Sbeity, 2014; Fernández et al., 2013; Khan, Azmi, Ansari, & Dhalvelkar, 2018; Liu et al., 2017b; Vitalij et al., 2012). The aim of the interventions is in many cases the more efficient use of resources (Al-Muaythir & Hossain, 2016; Hochstetler, Hochstetler, & Fu, 2016) but also the improvement of services through management and integration of different measures (Kunst, Avila, Pignaton, Bampi, & Rochol, 2018).

Table 8*: Interventions with the primary function to manage or integrate.*

Author (Year)	(Crime) Problem	Solution	Primary security function	Secondary security function
Khan et al. (2018)	Large quantities of call data records	Use of the call data records (CDRs) of various suspects and victims in order to extract significant evidence	manage	investigate
Dbouk et al. (2014)	Terrorist attacks	Surveillance system architecture	manage	
Bartoli et al. (2015)	Growing populations and demand to respond	Integrated platform for new generation professional mobile radio system, wireless sensor networks, social networks, and a data gathering and analysis system able to collect and elaborate heterogeneous information coming from different sources	manage	
Al-Muaythir and Hossain (2016)	Limited resources/inflexible systems	Parametric subscriptions/cloud-based publish/subscribe framework	manage	
Hochstetler et al. (2016)	Limited resources	Network of clusters to efficiently assign patrols based on informational entropy in order to minimise police time-to-arrival and the overall numbers of police on patrol	manage	
Lohokare, Dani, Sontakke, Apte, and Sahni (2017)	Response time	Capturing live location of the emergency services to connect them directly to nearest citizen in need	manage	
Duan, Lou, Wang, Gao, and Rui (2018)	Faults of static CCTV	AI oriented large-scale video management. Person/vehicle re-identification, facial recognition before coding	manage	
Hartama et al. (2017)	Emergency traffic management	Strategy related to efforts to improve the distribution of space and time based on traffic volume	manage	

Hosseini, Salehi, and Gottumukkala (2017)	Oversubscription of servers with relevant video feeds	Stream-priority aware resource allocation mechanism to enable interactive video prioritisation without a major impact on the flow of non-prioritised video streams	manage	
Patel, Wala, Shahu, and Lopes (2018)	Inefficient police records	Proposed online system for police stations which will help the policeman and user to digitalise their work.	manage	
Dey, Chakraborty, Naskar, and Misra (2012)	Faults of static CCTV	Multimedia surveillance backend system architecture based on the Sensor Web Enablement framework and cloud-based "key-value" stores	manage	improve
Chen et al. (2013)	Faults of static CCTV	New architectures integrated with Hadoop to resolve the urgent pressure of overloaded and to put the whole system into the computer cluster	manage	improve
Khorov, Gushchin, and Safonov (2015)	Faults of static CCTV	Easy implementation strategy to drop the smallest (in bytes) video frame whenever queue overflows	manage	improve
Lei et al. (2016)	Large quantities of data	K-means algorithm that can automatically split and merge clusters which incorporates the new ideas in dealing with huge scale of video data	manage	improve
Chen et al. (2016)	Faults of static CCTV	Dynamic video stream processing scheme to meet the requirements of real-time information processing and decision making	manage	improve
Pribadi, Kumiawan, Hariadi, and Nugroho (2017)	CCTV placement	Algorithm for improved camera placement.	manage	improve
Rametta, Baldoni, Lombardo, Micalizzi, and Vassallo (2017)	Faults of static CCTV	Smart CCTV platform to exploit the facilities offered by full SDN-NFV networks.	manage	improve
Liu and Lin (2017)	Automated license plate recognition	Hierarchical architecture combining supervised K-means and support vector machine.	manage	improve
Wu et al. (2017)	Data management in geographic information systems (GIS)	Hybrid database organization and management approach with SQL relational databases (RDB) and not only SQL (NoSQL) databases	manage	improve
Kunst et al. (2018)	High amounts of data traffic lessen the quality of service.	Multi-purpose real time video surveillance application using resource sharing	manage	improve
Duan et al. (2018)	Faults of static CCTV	Computational methodology for reorienting, repositioning, and merging camera positions within a region under surveillance.	manage	improve
Camboim et al. (2017)	Vehicle theft, violent crime on public transport	Smart surveillance system to recognise security threats in real time	manage	improve
Vitalij et al. (2012)	Lack of integration between different parts of smart cities.	Integrated framework with intelligent video surveillance, emergency communication, public address, general alarm/local notification systems, environmental monitoring and forecasting, local fire/chemical control systems, spotting, position location / eCall, ERA- GLONASS services, communications and mass media.	manage	improve

Liu et al. (2017b)	Integration of different data sources	Community safety oriented public information platform	manage	integrate
Fernández et al. (2013)	Vandalism prevention, perimeter security	Intelligent surveillance platform based on the use of large numbers of cheap sensors.	manage	detect

While it may at first seem as if the interventions collected in this category are not as relevant to security because they do not directly introduce new sensors or actuators (i.e. do not execute crime prevention tasks as such), they, in fact, take a central role in the security aspect of safe cities. This is especially relevant for safety and crime prevention planning and urban governance because larger quantities of information are transported and processed faster than before. This means not only that policies and decisions can rely on a more larger evidence base but also that decision making processes may need to change.

The integration of different security measures and their improved management through the implementation of connected systems is a prerequisite for the smart city (Ralko & Kumar, 2016). And because urban trends are heading in this direction, it is imperative that planners embrace the opportunities that come with it in all administrative procedures and planning processes to maintain the ability to solve urban problems in the future.

7.2.3 Section summary

Overall, many of the interventions clustered in this theme aim to enable smart city developments through the increased improvement and integration of city service infrastructure and its technological components. Despite this clear aim, the approaches taken in the literature differ substantially. While some studies approach smart city efforts on a micro-level (i.e. single layer), others propose holistic systems for the management of different services from sensors and processing units to actuators. This variety of approaches highlights the fact that smart city security infrastructure depends on integration on all levels, between and within the different parts of the surveillance and security apparatus (Hall et al., 2000).

This category of interventions is also crucial because it is most likely to be realised in practice. Only rarely are smart cities built from the ground up, and a more realistic path is the gradual improvement of existing systems (Mishra & Kumar, 2013). In this context, it is important to remember that smart security measures and the concept of the safe city are not born from the overwhelming failure of existing interventions but rather from the wish to improve existing efforts and to make them more efficient and manageable in the future (Truntsevsky, Lukiny, Sumachev, & Kopytova, 2018). As such, the interventions mentioned in this theme are not only practically appropriate, but they are also closest to the reality of financial and resource constraints in cities today. Given this it is surprising that only few studies (Al-Muaythir & Hossain, 2016; Hochstetler et al., 2016; Jun et al., 2017; Pereira et al., 2018) consider the economic implications or the financial efficiency of their interventions as a relevant factor in their deployment and evaluation. Despite the fact that efficiency and effectiveness are crucial factors in a smart city environment, we found many studies discussing operational efficiency in terms that were far from today's urban realities.

7.3 Entirely new functions

7.3.1 (Mass) information and crowdsourcing

While the original framework suggested an 'inform'-function limited to sounding alarm or alerting security services, this paper suggests that this definition should be revised. In total, this paper reviewed 13 studies that aimed to inform (i.e. communicate information about a specific situation) (Table 9). Only three of the interventions, however, functioned to automatically trigger actuators like alarming security services of a crime (Liu, Warade, Pai, & Gupta, 2017a; Mahajan et al., 2018; Nasui, Cernian, & Sgarciu, 2014). The other interventions were either user focussed on providing information about crime and crime prevention to the population (Ballesteros, Rahman, Carbunar, & Rishe, 2012; Kagawa, Saiki, & Nakamura, 2017; Mata et al., 2016; Peng, Xiao, Yao, Guan, & Yang, 2017; Truntsevsky et al., 2018) or fulfilled a hybrid role. To distinguish these two different groups, we will refer to the latter as 'mass information', while the former will be labelled as interventions with the aim to 'inform'. All of the studies are listed in table 9.

***Table 9**: Interventions with the primary function to crowdsource inform or provide mass-information.*

Author (Year)	(Crime) Problem	Solution	Primary security function	Secondary security function
Ballesteros et al. (2012)	Lack of awareness in dangerous situations	Combined use of personal mobile devices and social networks to make users aware of the safety of their surroundings.	(mass) inform	
Mata et al. (2016)	Mobile applications do not show safe routes	Approach to provide estimations defined by crime rates for generating safe routes in mobile devices.	(mass) inform	
Peng et al. (2017)	Safety indices for local areas are often inaccurate	Urban safety analysis system to infer safety index by leveraging multiple cross-domain urban data	(mass) inform	
Kagawa et al. (2017)	No information about security	PRISM (Personalized Real-time Information with Security Map)	(mass) inform	
Truntsevsky et al. (2018)	Street crime	Exploring the possible application of modern digital technologies in the evaluation and prevention of crime.	(mass) inform	
Arauz, Moreno, Nancalres, Pérez, and Larios (2017)	Corruption	Platform to integrate user orientation, application of standards for the development of the city and citizen participation.	inform	
Carreño, Gutierrez, Ochoa, and Fortino (2015)	Personal security	A mobile application which implements participatory sensing to help people be aware of the risks that appear to exist in a certain place at a certain time.	(mass) inform	
Moreira, Cacho, Lopes, and Cavalcante (2017)	Inefficient information for citizens	Mobile application as an alternative communication channel between public safety agencies and population.	inform	
Ferreira, Visintin, Okamoto, and Pu (2017)	Assaults and street crime	Smart surveillance cameras system, a back office system with a workflow engine and a mobile application within a collaborative concept	inform	
Bonatsos, Middleton, Melas, and Sabeur (2013)	Fear of crime/lack of awareness/misconceptions	Decision-support system integrating information, data and software modules representing city assets, hazards and processing models that simulate exposures to risks and potential compromise to safety and security.	inform	
Mahajan et al. (2018)	Assault, violence, attacks against women	Wearable/portable system that creates a sense of safety among women with a range of different features (automatic alarm, shock, audio streaming, location)	inform	
Nasui et al. (2014)	Transportation safety	Cloud based student transportation safety system is a location aware mobile asset management solution for operators of commercial fleets, having a cloud based platform at its core.	inform	detect
Liu et al. (2017a)	Street crime	Fine-grained location-aware smart campus security systems that leverages hybrid localisation approaches with minimum deployment cost.	inform	detect

Despite their different foci, both types of intervention increasingly involve the use of mobile applications to crowdsource information about criminal activity or public disorder. While some of these applications create a knowledge base that in turn aims to inform users (Carreño et al., 2015; Ferreira et al., 2017; Moreira et al., 2017), other applications, such as the online platform developed by Arauz et al. (2017), seek to tackle specific problems such as corruption by allowing users to report criminal activity directly to the authorities.

When assessing the effect these interventions have on the larger picture of urban security, it is important to distinguish between their different functions. While on one hand, mobile applications may be highly useful for mass information, i.e. to reach a large part of the population and to create broad awareness about crime and crime prevention, they also have downsides.

The most obvious issue of mobile applications is that their functionality and their ability to crowdsource information relies heavily on an active user base — without a crowd, no crowdsourcing. Even (or especially) if they are actively used, however, user-centric applications are open to misuse (Yang, Zhang, Ren, & Shen, 2015). Malicious actors may report false crimes to purposefully waste police resources or to put someone else in the crosshairs of security services. Another concern is that criminals could use apps just like the genuine user but to determine where victims might move to in order to avoid crime (Monahan & Mokos, 2013).

As discussed above, smart security technologies are aimed at making public services more efficient and effective and ultimately freeing up resources. This, however, is a double-edged sword, as 'inform'-functions make especially clear. While crowdsourcing information about crime with the goal of recording more crimes of a certain type can be considered an innovation on the sensor layer and may in some cases be desirable, it may in other cases put an unnecessary strain on already tight resources and overwhelm existing actuators. For example, an increased report rate for domestic abuse may very well save lives, but an app that floods police with hundreds of reports of anti-social behaviour or noise complaints may in the end take up disproportional amounts of resources (Elliott-

Davies, Donnelly, Boag-Munroe, & Van Mechelen, 2016). While interventions might be able to create a large network of 'eyes on the street' (Cozens & Davies, 2013; Hillier & Cozens, 2012), they may also create a flood of information that could overwhelm many public institutions.

Nevertheless, these interventions do offer some potential benefits. Especially crowd sourcing and mass information platforms can bring citizens and governments closer together (Kim & Lee, 2012). Not only can this help to streamline city services, but things like e-participation can also allow citizens to interact more directly with the administration of the place they live. This in turn can help to more directly include public opinion in planning processes and democratise the design and management of urban spaces (Macintosh, 2004).

Taking all of the above into account, it is difficult to assess the usefulness and impact of these interventions in terms of urban planning and governance as a whole. While elaborate measures of harm and police demand may give some indication of the usefulness of these interventions in terms of crime prevention, they largely ignore the overall usefulness across other realms (Greenfield & Paoli, 2013; Ratcliffe, 2015).

7.3.2 Predict

Predictive policing is in itself nothing new and has in the past grown to become one of the most well-researched realms in the field of policing. More recently, however, the wide-scale use of predictive policing has also come under intense scrutiny from both academics and practitioners (Brantingham, Valasik, & Mohler, 2018; Degeling & Berendt, 2017). Whether new technologies can revolutionise current approaches enough to make it a viable tool for policing without compromising privacy and data protection too much remains to be seen.

Nevertheless, this study has identified eight interventions that sought to provide security services with some form of predictive capabilities (Table 10).

***Table 10**: Interventions with some form of predictive capabilities.*

Author (Year)	(Crime) Problem	Solution	Primary security function	Secondary security function
Noor, Nawawi, and Ghazali (2013)	Prediction of situational crime factors	New tool that uses decision support system (DSS) and fuzzy association rule mining (FARM), in which it can extract the factors of situational (opportunity) crime	predict	
Oatley et al. (2015)	Faults of static CCTV	Utilising CCTV as a sensor to accurately model or give feedback on the reality of occurrences in digital space	predict	
Castelli et al. (2017)	Growing amounts of data	AI system for predicting violent crimes in urban areas starting from socio-economic and law-enforcement data	predict	
Garg, Malik, and Raj (2018)	Street crime	Gain insights into historical crime data to predict crimes	predict	
Catlett, Cesario, Talia, and Vinci (2018)	Forecasting inefficient	Predictive approach based on spatial analysis and auto-regressive models to automatically detect high-risk crime regions in urban areas and forecast crime	predict	
Isafiade and Bagula (2017)	Street crime	Crime series pattern detection	predict	
Araujo, Cacho, Thome, Medeiros, and Borges (2017)	Robbery and homicide	Smart city platform aimed at integrating several information systems from law enforcement agencies	predict	integrate
Kagawa, Saiki, and Nakamura (2018)	No information about crime in nearby area	Analyse street crimes according to users' living area using personalised security information service. Output is a crime map that helps citizens to avoid crime areas.	predict	warn

The extent and scope of these capabilities varied, however, greatly between the different interventions and reached from more traditional uses of historical crime data (Catlett et al., 2018; Garg et al., 2018; Noor et al., 2013) to the detection of psychopathy and potentially dangerous behaviour through CCTV and agent-based simulation through friendship networks on social media platforms (Oatley et al., 2015). What is new about many of these interventions is that their predictive capabilities include the real-time analysis of data as well as mechanisms for subsequent resource allocation, i.e. actuators. This separates them from current predictive policing tools which have been criticised for not being more accurate than an experienced police officer.

In addition, the growing importance of the online realm is reflected in a growing number of approaches. The model introduced by Oatley et al. (2015) emphasises that many people no longer express themselves actively in urban spaces but rather online, and that surveillance systems scanning crowds for suspicious behaviour only see half the picture (Oatley et al., 2015). This not only adds social media as a new dimension of urban surveillance, but it also forces a fundamental change in how we think about and plan for urban security.

7.3.3 Section summary

This section has introduced various interventions with functions that are not, or only to some extent, currently in use in policing and crime prevention. As such, they do not correspond to traditional functions of security interventions. While many of these interventions certainly offer great potential for transforming safe city designs and urban security landscapes, it is hard to evaluate the extent to which they will impact urban security as a whole due to the fast-paced nature of technological development. In addition, a lack of implementation cases and evaluative studies makes it impossible to predict what side-effects they may have (Siregar, Syahputra, Putra, & Wicaksono, 2018).

8. Conclusion

Our review introduced three categories of security interventions in smart cities. While some of the examined interventions did correspond with the traditional functions of security interventions both as sensors and actuators, we proposed a new classification for smart security interventions based on their functions.

Our classification distinguishes between three main categories, each with two sub-categories. The first category focussed on those interventions that combined new sensors with traditional actuators. This included interventions to detect and prevent unwanted criminal behaviour, and those aimed at identifying, authenticating, and defeating offenders. The second category included those interventions that sought to make old systems smart by either improving/automating processes or by managing and integrating the interplay between existing security solutions. The third category entailed those interventions that introduced entirely new functions such as (mass) information and crowd-sourcing as well as threat or crime prediction.

While this classification can help to group and compare interventions, they can also be useful to explore the distinct set of opportunities and challenges that they bring about. The proposed classification highlights that not all systems need to be fundamentally new to become smart and that building on existing infrastructure is crucial for a successful smartification. In addition, our analysis emphasises that the implications of the implementation of new security technologies in urban spaces are far-reaching with regards to urban planning and governance. Throughout, we show that future security infrastructures are not separate systems but reliant on and a prerequisite for the implementation of smart systems across other realms of city services. Especially the latter is important to consider for future smart city planning. Instead of treating security and crime prevention as the cherry on top of any smart city development, urban planners should consider it as a foundation. Not only do safety and security significantly impact if and how citizens interact with urban spaces but as shown in the discussion above, there are a variety of tools that can be used for citizen engagement across different realms of city services.

Overall, it is important to remember that smart security measures and the concept of the safe city are not born from the overwhelming failure of existing interventions but rather from the wish to improve existing efforts and to make them more efficient and manageable in the future. As such, they should be seen as a part of a larger holistic system that offers opportunities across all realms of city administration.

These opportunities do come, however, at a cost. The far-reaching implementation of smart technologies brings about new ethical considerations as well as implications for the planning process itself. Questions of data ownership and privacy rights grow in importance and need to be reflected in contemporary planning processes. In this review, we highlighted the importance of discussing these issues and criticised the lack of attention they have received in the smart city debate.

The question remains whether the use of such technologies will undermine individual privacy needs in the long run. Some authors stipulate that “surveillance technologies are a key component of smart and networked cities preventing or detecting crime and giving the residents a sense of safety" (van Heek, Aming, & Ziefle, 2016), while others such as Oatley et al. (2015)go as far as to describe CCTV networks as the fifth utility in smart cities. Yet while many innovations might create more efficient city services or effectively reduce crime, they might at the same time make people feel less secure because they have a sense that 'Big Brother' is watching. Particularly in authoritarian (or at least not fully democratic) regimes, the implementation of these new security measures can exponentially increase state power and control over its citizens. There is thus significant tension, as yet unresolved, between issues connected with these new technologies, especially with regards to privacy and data protection, and the importance of urban surveillance and security infrastructure for providing safety and security in the 21st century city.

Bibliography

Adey, P. (2002). Secured and Sorted Mobilities: Examples from the Airport. *Surveillance & Society, 1*(4).

Agha, A., Ranjan, R., & Gan, W.-S. (2017). Noisy vehicle surveillance camera: A system to deter noisy vehicle in smart city. *Applied Acoustics, 117*, 236-245.

Ahir, S., Kapadia, S., Chauhan, J., & Sanghavi, N. (2018). *The Personal Stun-A Smart Device For Women's Safety.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Al-Anbuky, A. (2014). *Sensor-actuator smart lighting system: system organizational concept and challenges.* Paper presented at the ICT for Sustainability 2014 (ICT4S-14).

Al-Muaythir, A., & Hossain, M. A. (2016). *Cloud-based parametrized publish/subscribe system for public safety applications in smarter cities.* Paper presented at the 2016 IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC).

Al-Shami, S., Zekri, A., El-Zaart, A., & Zantout, R. (2017). *On the parallelization of closed-set patterns classification for an automatic license plate recognition system.* Paper presented at the 2017 Sensors Networks Smart and Emerging Technologies (SENSET).

Alawadhi, S., Aldama-Nalda, A., Chourabi, H., Gil-Garcia, J. R., Leung, S., Mellouli, S., . . . Walker, S. (2012). *Building understanding of smart city initiatives.* Paper presented at the International conference on electronic government.

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology, 22*(1), 3-21.

Anagnostopoulos, T. (2014). *A Surveillance System for Preventing Suicide Attempts in Urban Metro Stations.* Paper presented at the Proceedings of the 18th Panhellenic Conference on Informatics.

Anees, V. M., & Kumar, G. S. (2017). *Direction estimation of crowd flow in surveillance videos.* Paper presented at the 2017 IEEE Region 10 Symposium (TENSYMP).

Ankitha, S., Nayana, K., Shravya, S., & Jain, L. (2017). *Smart city initiative: Traffic and waste management.* Paper presented at the Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on.

Araujo, A., Cacho, N., Thome, A. C., Medeiros, A., & Borges, J. (2017). *A predictive policing application to support patrol planning in smart cities.* Paper presented at the 2017 International Smart Cities Conference (ISC2).

Arauz, M. R., Moreno, Y., Nancalres, R., Pérez, C. V., & Larios, V. M. (2017). *Tackling corruption in urban development through open data and citizen empowerment: The case of "visor urbano" in guadalajara.* Paper presented at the 2017 International Smart Cities Conference (ISC2).

Baba, M., Pescaru, D., Gui, V., & Jian, I. (2016). *Stray dogs behavior detection in urban area video surveillance streams.* Paper presented at the 2016 12th IEEE International Symposium on Electronics and Telecommunications (ISETC).

Baldoni, G., Melita, M., Micalizzi, S., Rametta, C., Schembra, G., & Vassallo, A. (2017). *A dynamic, plug-and-play and efficient video surveillance platform for smart cities.* Paper presented at the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC).

Balla, P. B., & Jadhao, K. (2018). *IoT Based Facial Recognition Security System.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Ballesteros, J., Rahman, M., Carbunar, B., & Rishe, N. (2012). *Safe cities. A participatory sensing approach.* Paper presented at the 37th Annual IEEE Conference on Local Computer Networks.

Barba, C. T., Mateos, M. A., Soto, P. R., Mezher, A. M., & Igartua, M. A. (2012). *Smart city for VANETs using warning messages, traffic statistics and intelligent traffic lights.* Paper presented at the 2012 IEEE Intelligent Vehicles Symposium.

Bartoli, G., Fantacci, R., Gei, F., Marabissi, D., & Micciullo, L. (2015). A novel emergency management platform for smart public safety. *International Journal of Communication Systems, 28*(5), 928-943.

Bellini, P., Cenni, D., Nesi, P., & Paoli, I. (2017). Wi-Fi based city users' behaviour analysis for smart city. *Journal of Visual Languages & Computing, 42*, 31-45.

Belur, J., Tompson, L., Thornton, A., & Simon, M. (2018). Interrater reliability in systematic review methodology: exploring variation in coder decision-making. *Sociological methods & research*, 0049124118799372.

Benkő, M., & Germán, T. (2016). Crime prevention aspects of public space renewal in Budapest. *Journal of Place Management and Development, 9*(2), 191-209.

Berry, B. J. (2015). *The human consequences of urbanisation*: Macmillan International Higher Education.

Berry, M. (2018). Technology and organised crime in the smart city: an ethnographic study of the illicit drug trade. *City, Territory and Architecture, 5*(1), 16.

Bonatsos, A., Middleton, L., Melas, P., & Sabeur, Z. (2013). *Crime open data aggregation and management for the design of safer spaces in urban environments.* Paper presented at the International Symposium on Environmental Software Systems.

Borges, J., Ziehr, D., Beigl, M., Cacho, N., Martins, A., Sudrich, S., . . . Etter, M. (2017). *Feature engineering for crime hotspot detection.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Borrion, H., Ekblom, P., Alrajeh, D., Borrion, A. L., Keane, A., Koch, D., . . . Toubaline, S. (2019). The Problem with Crime Problem-Solving: Towards a Second Generation Pop? *The British Journal of Criminology*.

Borrion, H., Tripathi, K., Chen, P., & Moon, S. (2014). Threat detection: A framework for security architects and designers of metropolitan rail systems. *Urban, Planning and Transport Research, 2*(1), 173-194.

Boukerche, A., Siddiqui, A. J., & Mammeri, A. (2017). Automated Vehicle Detection and Classification: Models, Methods, and Techniques. *ACM Computing Surveys (CSUR), 50*(5), 62.

Bourmpos, M., Argyris, A., & Syvridis, D. (2014). Smart city surveillance through low-cost fiber sensors in metropolitan optical networks. *Fiber and Integrated Optics, 33*(3), 205-223.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*: Sage.

Brantingham, P. J., Valasik, M., & Mohler, G. O. (2018). Does predictive policing lead to biased arrests? Results from a randomized controlled trial. *Statistics and Public Policy, 5*(1), 1-6.

Braun, T., Fung, B. C., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable cities and society, 39*, 499-507.

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review, 82*(5), 977-1008.

Brust, M. R., Danoy, G., Bouvry, P., Gashi, D., Pathak, H., & Gonçalves, M. P. (2017). *Defending against intrusion of malicious uavs with networked uav defense swarms.* Paper presented at the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops).

Byun, J.-Y., Nasridinov, A., & Park, Y.-H. (2014). Internet of things for smart crime detection. *Contemporary Engineering Sciences, 7*(15), 749-754.

Cagliero, L., Cerquitelli, T., Chiusano, S., Garino, P., Nardone, M., Pralio, B., & Venturini, L. (2015). *Monitoring the citizens' perception on urban security in Smart City environments.* Paper presented at the 2015 31st IEEE International Conference on Data Engineering Workshops.

Calavia, L., Baladrón, C., Aguiar, J. M., Carro, B., & Sánchez-Esguevillas, A. (2012). A semantic autonomous video surveillance system for dense camera networks in smart cities. *Sensors, 12*(8), 10407-10429.

Camboim, H. B., Neto, A. J. V., Rodrigues, J. J., & Zhao, Z. (2017). *Applying Fog Computing to Improve Crime Assistance in Smart Transportation Safety Systems.* Paper presented at the 2017 IEEE First Summer School on Smart Cities (S3C).

Carreño, P., Gutierrez, F. J., Ochoa, S. F., & Fortino, G. (2015). Supporting personal security using participatory sensing. *Concurrency and Computation: Practice and Experience, 27*(10), 2531-2546.

Castella-Roca, J., Mut-Puigserver, M., Payeras-Capella, M. M., Viejo, A., & Angles-Tafalla, C. (2017). *Secure and Anonymous Vehicle Access Control System to Traffic-Restricted Urban Areas.* Paper presented at the 2017 26th International Conference on Computer Communication and Networks (ICCCN).

Castelli, M., Sormani, R., Trujillo, L., & Popovič, A. (2017). Predicting per capita violent crimes in urban areas: an artificial intelligence approach. *Journal of Ambient Intelligence and Humanized Computing, 8*(1), 29-36.

Catlett, C., Cesario, E., Talia, D., & Vinci, A. (2018). *A Data-Driven Approach for Spatio-Temporal Crime Predictions in Smart Cities.* Paper presented at the 2018 IEEE International Conference on Smart Computing (SMARTCOMP).

Cemgil, T., Kurutmaz, B., Cezayirli, A., Bingol, E., & Sener, S. (2017). *Interpolation and fraud detection on data collected by automatic meter reading.* Paper presented at the 2017 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG).

Chackravarthy, S., Schmitt, S., & Yang, L. (2018). *Intelligent Crime Anomaly Detection in Smart Cities Using Deep Learning.* Paper presented at the 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC).

Chen, N., Chen, Y., You, Y., Ling, H., Liang, P., & Zimmermann, R. (2016). *Dynamic urban surveillance video stream processing using fog computing.* Paper presented at the 2016 IEEE second international conference on multimedia big data (BigMM).

Chen, X., Xu, J.-B., & Guo, W.-Q. (2013). *The research about video surveillance platform based on cloud computing.* Paper presented at the 2013 International Conference on Machine Learning and Cybernetics.

Cho, Y. I. (2012). *Designing smart cities: Security issues.* Paper presented at the IFIP International Conference on Computer Information Systems and Industrial Management.

Cocchia, A. (2014). Smart and digital city: A systematic literature review *Smart city* (pp. 13-43): Springer.

Cozens, P., & Davies, T. (2013). Crime and residential security shutters in an Australian suburb: Exploring perceptions of 'Eyes on the Street', social interaction and personal safety. *Crime prevention and community safety, 15*(3), 175-191.

Cubik, J., Kepak, S., Nedoma, J., Fajkus, M., Zboril, O., Novak, M., . . . Vasinek, V. (2017). *Fiber optic perimeter system for security in smart city.* Paper presented at the Electro-Optical Remote Sensing XI.

Datta, S., & Sarkar, S. (2017). *Automation, security and surveillance for a smart city: Smart, digital city.* Paper presented at the 2017 IEEE Calcutta Conference (CALCON).

Dbouk, M., Mcheick, H., & Sbeity, I. (2014). CityPro; An integrated city-protection collaborative platform. *Procedia Computer Science, 37*, 72-79.

de Diego, I. M., San Román, I., Montero, J. C., Conde, C., & Cabello, E. (2018). Scalable and flexible wireless distributed architecture for intelligent video surveillance systems. *Multimedia Tools and Applications*, 1-23.

de Kort, Y., IJsselsteijn, W., Haans, A., Lakens, D., Kalinauskaite, I., & Schietecat, A. (2014). *De-escalate: Defusing escalating behaviour through the use of interactive light scenarios.* Paper presented at the Proc. Experiencing Light.

Degeling, M., & Berendt, B. (2017). What is wrong about Robocops as consultants? A technology-centric critique of predictive policing. *AI & SOCIETY*, 1-10.

Dey, S., Chakraborty, A., Naskar, S., & Misra, P. (2012). *Smart city surveillance: Leveraging benefits of cloud data stores.* Paper presented at the 37th Annual IEEE Conference on Local Computer Networks-Workshops.

Duan, L., Lou, Y., Wang, S., Gao, W., & Rui, Y. (2018). AI oriented large-scale video management for smart city: Technologies, standards and beyond. *IEEE MultiMedia*.

Durga, S., Surya, S., & Daniel, E. (2018). *SmartMobiCam: Towards a New Paradigm for Leveraging Smartphone Cameras and IaaS Cloud for Smart City Video Surveillance.* Paper presented at the 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI).

Eigenraam, D., & Rothkrantz, L. (2016). *A smart surveillance system of distributed smart multi cameras modelled as agents.* Paper presented at the 2016 Smart Cities Symposium Prague (SCSP).

Ekblom, P., & Hirschfield, A. (2014). Developing an alternative formulation of SCP principles–the Ds (11 and counting). *Crime Science, 3*(1), 2.

Elliott-Davies, M., Donnelly, J., Boag-Munroe, F., & Van Mechelen, D. (2016). 'Getting a battering' The perceived impact of demand and capacity imbalance within the Police Service of England and Wales: A qualitative review. *The Police Journal, 89*(2), 93-116.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research, 5*(4), 491-497.

Ertugrul, E., Kocaman, U., & Sahingoz, O. K. (2018). *Autonomous aerial navigation and mapping for security of smart buildings.* Paper presented at the 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG).

Federici, J. F., Schulkin, B., Huang, F., Gary, D., Barat, R., Oliveira, F., & Zimdars, D. (2005). THz imaging and sensing for security applications—explosives, weapons and drugs. *Semiconductor Science and Technology, 20*(7), S266.

Feng, G. C. (2014). Intercoder reliability indices: disuse, misuse, and abuse. *Quality & Quantity, 48*(3), 1803-1815.

Fernández, J., Calavia, L., Baladrón, C., Aguiar, J., Carro, B., Sánchez-Esguevillas, A., . . . Smilansky, Z. (2013). An intelligent surveillance platform for large metropolitan areas with dense sensor deployment. *Sensors, 13*(6), 7414-7442.

Ferreira, J. E., Visintin, J. A., Okamoto, J., & Pu, C. (2017). *Smart services: A case study on smarter public safety by a mobile app for University of São Paulo.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Filipponi, L., Vitaletti, A., Landi, G., Memeo, V., Laura, G., & Pucci, P. (2010). *Smart city: An event driven architecture for monitoring public spaces with heterogeneous sensors.* Paper presented at the 2010 Fourth International Conference on Sensor Technologies and Applications.

García, C. G., Meana-Llorián, D., G-Bustelo, B. C. P., Lovelle, J. M. C., & Garcia-Fernandez, N. (2017). Midgar: Detection of people through computer vision in the Internet of Things scenarios to improve the security in Smart Cities, Smart Towns, and Smart Homes. *Future Generation Computer Systems, 76*, 301-313.

García, R. O., Valentín, L., Serrano, S. A., Palacios-Alonso, M. A., & Sucar, L. E. (2017). GEOVISUALIZATION FOR SMART VIDEO SURVEILLANCE. *ISPRS Annals of Photogrammetry, Remote Sensing & Spatial Information Sciences, 4*.

Garg, R., Malik, A., & Raj, G. (2018). *A Comprehensive Analysis for Crime Prediction in Smart City Using R Programming.* Paper presented at the 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence).

Gaur, A., Scotney, B., Parr, G., & McClean, S. (2015). Smart city architecture and its applications based on IoT. *Procedia Computer Science, 52*, 1089-1094.

Giyenko, A., & Im Cho, Y. (2016). *Intelligent UAV in smart cities using IoT.* Paper presented at the 2016 16th International Conference on Control, Automation and Systems (ICCAS).

Gohar, M., Muzammal, M., & Rahman, A. U. (2018). SMART TSS: Defining transportation system behavior using big data analytics in smart cities. *Sustainable cities and society, 41*, 114-119.

Gough, D., Oliver, S., & Thomas, J. (2017). *An introduction to systematic reviews*: Sage.

Greenfield, V. A., & Paoli, L. (2013). A framework to assess the harms of crimes. *British Journal of Criminology, 53*(5), 864-885.

Gupta, A., Chakraborty, N., & Mondal, S. (2017). *CETD: An efficient clustering based energy theft detection technique in smart grid.* Paper presented at the 2017 IEEE Region 10 Symposium (TENSYMP).

Habibzadeh, H., Soyata, T., Kantarci, B., Boukerche, A., & Kaptan, C. (2018). Sensing, communication and security planes: A new challenge for a smart city system design. *Computer Networks, 144*, 163-200.

Hadjkacem, B., Ayedi, W., Abid, M., & Snoussi, H. (2017). *A new method of video-surveillance data analytics for the security in camera networks.* Paper presented at the 2017 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC).

Hall, R. E., Bowerman, B., Braverman, J., Taylor, J., Todosow, H., & Von Wimmersperg, U. (2000). *The vision of a smart city*.

Hardmeier, D., Hofer, F., & Schwaninger, A. (2005). *The X-ray object recognition test (X-ray ORT)-a reliable and valid instrument for measuring visual abilities needed in X-ray screening.* Paper presented at the Security Technology, 2005. CCST'05. 39th Annual 2005 International Carnahan Conference on.

Hartama, D., Mawengkang, H., Zarlis, M., Sembiring, R. W., Furqan, M., Abdullah, D., & Rahim, R. (2017). *A research framework of disaster traffic management to Smart City.* Paper presented at the 2017 Second International Conference on Informatics and Computing (ICIC).

Hillier, D., & Cozens, P. (2012). Revisiting Jane Jacobs's 'Eyes on the Street'for the Twenty-First Century: Evidence from Environmental Criminology *The Urban Wisdom of Jane Jacobs* (pp. 202-220): Routledge.

Hochstetler, J., Hochstetler, L., & Fu, S. (2016). *An optimal police patrol planning strategy for smart city safety.* Paper presented at the 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on

Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS).

Hosseini, M., Salehi, M. A., & Gottumukkala, R. (2017). *Enabling interactive video streaming for public safety monitoring through batch scheduling.* Paper presented at the 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS).

Hu, L., & Ni, Q. (2018). IoT-driven automated object detection algorithm for urban surveillance systems in smart cities. *IEEE Internet of Things Journal, 5*(2), 747-754.

Huang, P.-R., & Chu, E. T.-H. (2017). *Indoor trapped-victim detection system.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Isafiade, O. E., & Bagula, A. B. (2017). *Fostering smart city development in developing nations: A crime series data analytics approach.* Paper presented at the 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K).

Jalali, R., El-Khatib, K., & McGregor, C. (2015). *Smart city architecture for community level services through the internet of things.* Paper presented at the 2015 18th International Conference on Intelligence in Next Generation Networks.

Jun, S., Chang, T.-W., Jeong, H., & Lee, S. (2017). Camera Placement in Smart Cities for Maximizing Weighted Coverage with Budget Limit. *IEEE Sensors Journal, 17*(23), 7694-7703.

Kagawa, T., Saiki, S., & Nakamura, M. (2017). *Developing personalized security information service using open data.* Paper presented at the 2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD).

Kagawa, T., Saiki, S., & Nakamura, M. (2018). Analyzing street crimes in Kobe city using PRISM. *International Journal of Web Information Systems*.

Khan, E. S., Azmi, H., Ansari, F., & Dhalvelkar, S. (2018). *Simple Implementation of Criminal Investigation using Call Data Records (CDRs) through Big Data Technology.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Khorov, E., Gushchin, A., & Safonov, A. (2015). *Distortion Avoidance While Streaming Public Safety Video in Smart Cities.* Paper presented at the International Workshop on Multiple Access Communications.

Kim, S., & Lee, J. (2012). E-participation, transparency, and trust in local government. *Public Administration Review, 72*(6), 819-828.

Kirschenbaum, A. A., Mariani, M., Van Gulijk, C., Rapaport, C., & Lubasz, S. (2012). Airports at risk: the impact of information sources on security decisions. *Journal of Transportation Security, 5*(3), 187-197.

Kumar, S., Datta, D., Singh, S. K., & Sangaiah, A. K. (2018). An intelligent decision computing paradigm for crowd monitoring in the smart city. *Journal of Parallel and Distributed Computing, 118*, 344-358.

Kunst, R., Avila, L., Pignaton, E., Bampi, S., & Rochol, J. (2018). Improving network resources allocation in smart cities video surveillance. *Computer Networks, 134*, 228-244.

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *biometrics*, 159-174.

Lee, H., Smeaton, A. F., O'Connor, N., & Murphy, N. (2005). User-interface to a CCTV video search system.

Lei, J., Jiang, T., Wu, K., Du, H., Zhu, G., & Wang, Z. (2016). Robust K-means algorithm with automatically splitting and merging clusters and its applications for surveillance data. *Multimedia Tools and Applications, 75*(19), 12043-12059.

Lella, J., Mandla, V. R., & Zhu, X. (2017). Solid waste collection/transport optimization and vegetation land cover estimation using Geographic Information System (GIS): A case study of a proposed smart-city. *Sustainable cities and society, 35*, 336-349.

Liu, K., Warade, N., Pai, T., & Gupta, K. (2017a). *Location-aware smart campus security application.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Liu, S., Ni, L. M., & Krishnan, R. (2014). Fraud detection from taxis' driving behaviors. *IEEE Transactions on Vehicular Technology, 63*(1), 464-472.

Liu, W.-C., & Lin, C.-H. (2017). *A hierarchical license plate recognition system using supervised K-means and Support Vector Machine.* Paper presented at the 2017 International Conference on Applied System Innovation (ICASI).

Liu, Y., Yu, L., Chi, T., Yang, B., Yao, X., Yang, L., . . . Cui, S. (2017b). *Design and implementation of community safety management oriented public information platform for a smart city.* Paper presented at the 2017 Forum on Cooperative Positioning and Service (CPGPS).

Lohokare, J., Dani, R., Sontakke, S., Apte, A., & Sahni, R. (2017). *Emergency services platform for smart cities.* Paper presented at the 2017 IEEE Region 10 Symposium (TENSYMP).

Ma, X., He, Y., Luo, X., Li, J., Zhao, M., An, B., & Guan, X. (2018). Camera Placement Based on Vehicle Traffic for Better City Security Surveillance. *IEEE Intelligent Systems, 33*(4), 49-61.

Macintosh, A. (2004). *Characterizing e-participation in policy-making.* Paper presented at the 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the.

Mahajan, M., Reddy, K., & Rajput, M. (2018). *A Switch Triggered Rescue Assistance System for Safety of Women.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Manasa, N. (2016). *Nano Sensors and Pattern Recognition for Detection of Hidden Explosives.* Paper presented at the Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies.

Marx, G. T. (1998). Ethics for the new surveillance. *The Information Society, 14*(3), 171-185.

Mata, F., Torres-Ruiz, M., Guzmán, G., Quintero, R., Zagal-Flores, R., Moreno-Ibarra, M., & Loza, E. (2016). A mobile information system based on crowd-sensed and official crime data for finding safe routes: A case study of mexico city. *Mobile Information Systems, 2016*.

McCoy, T., Bullock, R., & Brennan, P. (2005). RFID for airport security and efficiency.

McLeod, S. (2007). Maslow's hierarchy of needs. *Simply psychology, 1*.

Mehboob, F., Abbas, M., Rehman, S., Khan, S. A., Jiang, R., & Bouridane, A. (2017). Glyph-based video visualization on Google Map for surveillance in smart cities. *EURASIP Journal on Image and Video Processing, 2017*(1), 28.

Memos, V. A., Psannis, K. E., Ishibashi, Y., Kim, B.-G., & Gupta, B. B. (2018). An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. *Future Generation Computer Systems, 83*, 619-628.

Miraftabzadeh, S. A., Rad, P., Choo, K.-K. R., & Jamshidi, M. (2018). A Privacy-Aware Architecture at the Edge for Autonomous Real-Time Identity Reidentification in Crowds. *IEEE Internet of Things Journal, 5*(4), 2936-2946.

Mishra, D., & Kumar, M. (2013). Role of Technology in Smart Governance:'Smart City, Safe City'. *Safe City'(August 15, 2013)*.

Mlinarić, A., Horvat, M., & Šupak Smolčić, V. (2017). Dealing with the positive publication bias: Why you should really publish your negative results. *Biochemia medica: Biochemia medica, 27*(3), 1-6.

Monahan, T., & Mokos, J. T. (2013). Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. *Geoforum, 49*, 279-288.

Moreira, B., Cacho, N., Lopes, F., & Cavalcante, E. (2017). *Towards civic engagement in smart public security.* Paper presented at the 2017 International Smart Cities Conference (ISC2).

Morton, P. J., Horne, M., Dalton, R. C., & Thompson, E. M. (2012). Virtual city models: Avoidance of obsolescence. *Education and Research in Computer Aided Architectural Design in Europe-eCAADe, 1*, 213-224.

Naphade, M., Banavar, G., Harrison, C., Paraszczak, J., & Morris, R. (2011). Smarter cities and their innovation challenges. *Computer, 44*(6), 32-39.

Nasui, D., Cernian, A., & Sgarciu, V. (2014). *Cloud based Student Transportation Safety System.* Paper presented at the Proceedings of the 2014 6th International Conference on Electronics, Computers and Artificial Intelligence (ECAI).

Noor, N. M. M., Nawawi, W. M. F. W., & Ghazali, A. F. (2013). *Supporting decision making in situational crime prevention using fuzzy association rule.* Paper presented at the 2013 International Conference on Computer, Control, Informatics and Its Applications (IC3INA).

Oatley, G., Crick, T., & Bolt, D. (2015). *CCTV as a smart sensor network.* Paper presented at the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing.

Olive, E. W., Laube, R., & Hofer, F. (2009). *A comparison between two leadership models for security checkpoints.* Paper presented at the Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on.

Oza, N., & Gohil, N. (2016). *Implementation of cloud based live streaming for surveillance.* Paper presented at the 2016 International Conference on Communication and Signal Processing (ICCSP).

Parra, J., & Lopez, R. (2017). Application of predictive analytics for crime prevention: The case of the City of San Francisco *Police: Global Perceptions, Performance and Ethical Challenges* (pp. 85-109): Nova Science Publishers, Inc.

Patel, J., Wala, H., Shahu, D., & Lopes, H. (2018). *Intellectual and Enhance Digital Solution For Police Station.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Patton, J. W. (2000). Protecting privacy in public? Surveillance technologies and the value of public places. *Ethics and Information Technology, 2*(3), 181-187.

Peixoto, M. L., Souza, I., Barbosa, M., Lecomte, G., Batista, B. G., Kuehne, B. T., & Leite Filho, D. M. (2018). *Data Missing Problem in Smart Surveillance Environment.* Paper presented at the 2018 International Conference on High Performance Computing & Simulation (HPCS).

Peng, Z., Xiao, B., Yao, Y., Guan, J., & Yang, F. (2017). *U-safety: Urban safety analysis in a smart city.* Paper presented at the 2017 IEEE International Conference on Communications (ICC).

Pereira, R., Correia, D., Mendes, L., Rabadão, C., Barroso, J., & Pereira, A. (2018). *Low-Cost Smart Surveillance System for Smart Cities.* Paper presented at the International Conference on Universal Access in Human-Computer Interaction.

Pribadi, A., Kumiawan, F., Hariadi, M., & Nugroho, S. M. S. (2017). *Urban distribution CCTV for smart city using decision tree methods.* Paper presented at the 2017 International Seminar on Intelligent Technology and Its Applications (ISITIA).

Ralko, S., & Kumar, S. (2016). Smart City Security.

Ramaprasad, A., Sánchez-Ortiz, A., & Syn, T. (2017). *A unified definition of a smart city.* Paper presented at the International Conference on Electronic Government.

Rametta, C., Baldoni, G., Lombardo, A., Micalizzi, S., & Vassallo, A. (2017). S6: a Smart, Social and SDN-based Surveillance System for Smart-cities. *Procedia Computer Science, 110*, 361-368.

Ramírez, C. A., Barragán, R., García-Torales, G., & Larios, V. M. (2016). *Low-power device for wireless sensor network for Smart Cities.* Paper presented at the 2016 IEEE MTT-S Latin America Microwave Conference (LAMC).

Ratcliffe, J. H. (2015). Towards an index for harm-focused policing. *Policing: A journal of policy and practice, 9*(2), 164-182.

Rathore, M. M., Ahmad, A., Paul, A., & Rho, S. (2016). Urban planning and building smart cities based on the internet of things using big data analytics. *Computer Networks, 101*, 63-80.

Reddy, A. G., Suresh, D., Phaneendra, K., Shin, J. S., & Odelu, V. (2018a). Provably secure pseudo-identity based device authentication for smart cities environment. *Sustainable cities and society, 41*, 878-885.

Reddy, K. B. S., Loke, O., Jani, S., & Dabre, K. (2018b). *Tracking People In Real Time Video Footage Using Facial Recognition.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Rocher, J., Taha, M., Parra, L., & Lloret, J. (2018). *IoT Sensor to Detect Fraudulent Use of Dyed Fuels in Smart Cities.* Paper presented at the 2018 Fifth International Conference on Internet of Things: Systems, Management and Security.

Rohstein, H., & Hopewell, S. (2009). Grey Literature. In H. Cooper, L. V. Hedges, & J. Valentine (Eds.), *Handbook of Research on Adult Learning and Development* (2nd ed., pp. 184-202): Routledge.

Rothkrantz, L. (2017a). *Lip-reading by surveillance cameras.* Paper presented at the 2017 Smart City Symposium Prague (SCSP).

Rothkrantz, L. (2017b). *Person identification by smart cameras.* Paper presented at the 2017 Smart City Symposium Prague (SCSP).

Saba, A. (2017). *IOT based energy efficient security system.* Paper presented at the 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT).

Sadgali, I., Sael, N., & Benabbou, F. (2018). Detection of credit card fraud: State of art. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY, 18*(11), 76-83.

Sajjad, M., Nasir, M., Muhammad, K., Khan, S., Jan, Z., Sangaiah, A. K., . . . Baik, S. W. (2017). Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. *Future Generation Computer Systems*.

Sajjad, M., Nasir, M., Ullah, F. U. M., Muhammad, K., Sangaiah, A. K., & Baik, S. W. (2018). Raspberry Pi assisted facial expression recognition framework for smart security in law-enforcement services. *Information Sciences, 479*, 416-431.

Salmerón-García, J. J., van den Dries, S., Díaz-del-Río, F., Morgado-Estevez, A., Sevillano-Ramos, J. L., & van de Molengraft, M. (2017). Towards a cloud-based automated surveillance system using wireless technologies. *Multimedia Systems*, 1-15.

Sandborn, P. (2007). *Designing for technology obsolescence management.* Paper presented at the IIE Annual Conference. Proceedings.

Saravanakumar, K., Deepa, K., & Kumar, N. S. (2017). *A study on possible application of RFID system in different real-time environments.* Paper presented at the 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT).

Schuilenburg, M., & Peeters, R. (2018). Smart cities and the architecture of security: pastoral power and the scripted design of public space. *City, Territory and Architecture, 5*(1), 13.

Shi, J., Ming, Y., Fan, C., & Tian, L. (2017). *Face recognition algorithm based on multi-scale CLBP.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Singh, A., Patil, D., & Omkar, S. (2018). Eye in the Sky: Real-time Drone Surveillance System (DSS) for Violent Individuals Identification using ScatterNet Hybrid Deep Learning Network. *arXiv preprint arXiv:1806.00746*.

Singh, G., Majumdar, S., & Rajan, S. (2017). *MapReduce-based techniques for multiple object tracking in video analytics.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Siregar, A. H., Syahputra, D., Putra, D. A., & Wicaksono, B. (2018). *Policy Evaluation of Security System Based on Security Camera Technology in Batam City.* Paper presented at the IOP Conference Series: Earth and Environmental Science.

Sormani, R., Soldatos, J., Vassilaras, S., Kioumourtzis, G., Leventakis, G., Giordani, I., & Tisato, F. (2016). A serious game empowering the prediction of potential terrorist actions. *Journal of Policing, Intelligence and Counter Terrorism, 11*(1), 30-48.

Sudha, N. (2015). *Enabling Seamless Video Processing in Smart Surveillance Cameras with Multicore.* Paper presented at the 2015 International Conference on Advanced Computing and Communications (ADCOM).

Sweet, K. (2008). *Aviation and airport security: terrorism and safety concerns*: CRC Press.

Tan, H., & Chen, L. (2014). *An approach for fast and parallel video processing on Apache Hadoop clusters.* Paper presented at the 2014 IEEE International Conference on Multimedia and Expo (ICME).

Thomas, J., O'Mara-Eves, A., Harden, A., & Newman, M. (2017a). Synthesis Methods for Combining and Configuring Quantitative Data. In D. Gough, S. Oliver, & J. Thomas (Eds.), *An Introduction to Systematic Reviews* (2nd ed., pp. 181-211). London: SAGE Publications.

Thomas, S. S., Gupta, S., & Subramanian, V. K. (2017b). *Smart surveillance based on video summarization.* Paper presented at the 2017 IEEE Region 10 Symposium (TENSYMP).

Tian, L., Wang, H., Zhou, Y., & Peng, C. (2018). Video big data in smart city: Background construction and optimization for surveillance video processing. *Future Generation Computer Systems, 86*, 1371-1382.

Truntsevsky, Y. V., Lukiny, I., Sumachev, A., & Kopytova, A. (2018). *A smart city is a safe city: the current status of street crime and its victim prevention using a digital application.* Paper presented at the MATEC Web of Conferences.

Valentín, L., Serrano, S. A., García, R. O., Andrade, A., Palacios-Alonso, M. A., & Sucar, L. E. (2017). A CLOUD-BASED ARCHITECTURE FOR SMART VIDEO SURVEILLANCE. *International Archives of the Photogrammetry, Remote Sensing & Spatial Information Sciences, 42*.

van Heek, J., Aming, K., & Ziefle, M. (2016). *"How fear of crime affects needs for privacy & safety": Acceptance of surveillance technologies in smart cities.* Paper presented at the Smart Cities and Green ICT Systems (SMARTGREENS), 2016 5th International Conference on.

Venkatesan, S., Jawahar, A., Varsha, S., & Roshne, N. (2017). *Design and implementation of an automated security system using Twilio messaging service.* Paper presented at the 2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS).

Viera, A. J., & Garrett, J. M. (2005). Understanding interobserver agreement: the kappa statistic. *Fam med, 37*(5), 360-363.

Vitalij, F., Robnik, A., & Alexey, T. (2012). " Safe City"-an Open and Reliable Solution for a Safe and Smart City. *Elektrotehniski Vestnik, 79*(5), 262.

Wang, J., Pan, J., & Esposito, F. (2017). *Elastic urban video surveillance system using edge computing.* Paper presented at the Proceedings of the Workshop on Smart Internet of Things.

Welsh, D., & Roy, N. (2017). *Smartphone-based mobile gunshot detection.* Paper presented at the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops).

Wilson, D. B. (2009). Missing a critical piece of the pie: simple document search strategies inadequate for systematic reviews. *Journal of experimental criminology, 5*(4), 429-440.

Wu, C., Zhu, Q., Zhang, Y., Du, Z., Ye, X., Qin, H., & Zhou, Y. (2017). A NOSQL–SQL hybrid organization and management approach for real-time geospatial data: A case study of public security video surveillance. *ISPRS International Journal of Geo-Information, 6*(1), 21.

Xiong, M., Chen, D., Chen, J., Chen, J., Shi, B., Liang, C., & Hu, R. (2017). Person re-identification with multiple similarity probabilities using deep metric learning for efficient smart security applications. *Journal of Parallel and Distributed Computing*.

Xu, Z., Mei, L., Liu, Y., Hu, C., & Chen, L. (2016). Semantic enhanced cloud environment for surveillance data management using video structural description. *Computing, 98*(1-2), 35-54.

Yang, K., Zhang, K., Ren, J., & Shen, X. (2015). Security and privacy in mobile crowdsourcing networks: challenges and opportunities. *IEEE communications magazine, 53*(8), 75-81.

Zhang, C., Ni, B., Song, L., Zhai, G., Yang, X., & Zhang, W. (2016). *BEST: benchmark and evaluation of surveillance task.* Paper presented at the Asian Conference on Computer Vision.

Zhang, F., Wan, M., Yang, G., & Yang, Z. (2017a). *Background modeling from surveillance video via transformed L 1 function.* Paper presented at the 2017 International Smart Cities Conference (ISC2).

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017b). Security and privacy in smart city applications: Challenges and solutions. *IEEE communications magazine, 55*(1), 122-129.

Zhang, S., & Yu, H. (2018). Person Re-Identification by Multi-Camera Networks for Internet of Things in Smart Cities. *IEEE Access, 6*, 76111-76117.

Zhang, T., Chowdhery, A., Bahl, P. V., Jamieson, K., & Banerjee, S. (2015). *The design and implementation of a wireless video surveillance system.* Paper presented at the Proceedings of the 21st Annual International Conference on Mobile Computing and Networking.

Zheng, Y., Sheng, H., Zhang, B., Zhang, J., & Xiong, Z. (2015). Weight-based sparse coding for multi-shot person re-identification. *Science China Information Sciences, 58*(10), 1-15.

Zhou, W., Saha, D., & Rangarajan, S. (2015). *A system architecture to aggregate video surveillance data in Smart Cities.* Paper presented at the 2015 IEEE Global Communications Conference (GLOBECOM).

Zhu, S., Li, D., & Feng, H. (2019). Is smart city resilient? Evidence from China. *Sustainable cities and society*, 101636.

Zingoni, A., Diani, M., & Corsini, G. (2017). A flexible algorithm for detecting challenging moving objects in real-time within IR video sequences. *Remote Sensing, 9*(11), 1128.

Zygiaris, S. (2013). Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems. *Journal of the knowledge economy, 4*(2), 217-231.