VARSTVOSLOVJE,
Journal of Criminal
Justice and Security,
year 20
no. 4
pp. 389–413

Analysis of the Relationship Between Smart Cities, Policing and Criminal Investigation

Kaja Prislan, Boštjan Slak

A gunshot rings out in a high-crime section of a large city. A car speeds away. A victim lies on the sidewalk. An audio sensor embedded in a nearby streetlamp detects the sound of gunfire, identifies where it came from and, through a high-speed backhaul to the nearest real-time crime center, alerts dispatchers to the situation. As police and emergency medical technicians race to the scene, the streetlight brightens to its full capacity, making it easier for first responders to see what's going on. Behind the scenes, the feeds collected by the surveillance cameras automatically are run through databases housing fingerprint, DNA and mugshot information. Real-time license plate and facial recognition technologies are applied, and a data analytics engine kicks in to correlate the data and provide actionable intelligence. The result? The perpetrators can be more quickly captured by law enforcement.

(Pillaipakkam, 2017, pp. 33–34)

Purpose:

The main objective is to present the symbiosis between smart cities, policing, criminal investigation and criminal intelligence. Moreover, another purpose is to critically address the underlying privacy concerns arising from smart city designs.

Design/Methods/Approach:

The paper is theoretical in scope and utilises a literature review as the basic method. Correlations between smart cities, policing and criminal investigations are identified by analysing the applicability of core smart city technologies and services [SCTS].

Findings:

It is evident that SCTS can influence policing styles and police effectiveness. SCTS hold great potential for criminal investigations and criminal intelligence as they provide information upon which police can develop investigations or crime-control strategies. Vice-versa, criminal investigations and criminal intelligence can provide guidelines for SCTS developers and the governance of smart cities. However, privacy concerns and the slowly developing regulatory framework remain the biggest issues when it comes to SCTS adoption, thus making measures to safeguard privacy a key factor for the legitimacy of smart cities and smart policing.

Practical Implications:

The paper introduces practical knowledge about the implications of smart cities for policing and crime investigation. Some research ideas are presented as

well as suggestions for legislators, developers and others whose work area falls in the scope of (smart) city governance.

Originality/Value:

A comprehensive study of the symbiosis between smart cities and policing must not only consider the potential of SCTS but the related need to develop regulation and skillsets of human resources. Only a handful of papers address the connectivity of smart cities, criminal investigations and criminal intelligence from such a multidisciplinary scope. Therefore, the paper represents a contribution to works discussing these concepts.

UDC: 351.78:004.7

Keywords: smart cities, safety and security provision, policing, criminal investigation, criminal intelligence

Analiza povezanosti pametnih mest s policijsko in kriminalistično dejavnostjo

Namen prispevka:

Namen prispevka je predstaviti simbiozo med pametnimi mesti, policijsko dejavnostjo, kriminalističnim preiskovanjem in kriminalističnoobveščevalno dejavnostjo. V tem kontekstu je podan tudi kritični razmislek o izzivih in dilemah, povezanih z varstvom zasebnosti.

Metode:

Prispevek je teoretične narave in temelji na pregledu literature. Korelacije med temeljnimi pojmi (pametna mesta, policijska in kriminalistična dejavnost) smo identificirali z analizo temeljnih tehnologij, sistemov in storitev, ki podpirajo delovanje pametnih mest.

Ugotovitve:

Tehnologije pametnih mest omogočajo razvoj novih oblik policijskega dela in imajo potencial za izboljšanje policijske učinkovitosti. Funkcionalnost tehnologij je razvidna tudi na področju kriminalistične dejavnosti, ki lahko z obdelovanjem podatkov in njihovo uporabo bolje načrtuje kriminalistične preiskave in razvija strategije preprečevanja kriminalitete. Simbioza je opazna tudi z nasprotnega vidika – s podajanjem smernic lahko kriminalistična in policijska dejavnost pomagata upravljavcem pametnih mest in razvojnikom tehnologij ter rešitev. Glavni izziv predstavlja varovanje zasebnosti in osebnih podatkov prebivalcev, zato so mehanizmi za preprečevanje zlorab ključni faktor legitimnosti pametnih mest in policijske dejavnosti.

Praktična uporabnost:

V prispevku so predstavljena uporabna znanja glede potencialov pametnih mest za izvajanje policijske in kriminalistične dejavnosti, prav tako tudi predlogi za raziskovalce in oblikovalce politik, razvojnike in druge, ki delujejo na področju upravljanja (pametnih) mest.

Izvirnost/pomembnost prispevka:

Če želimo razumeti sistem dejavnikov, ki vplivajo na simbiozo med policijsko dejavnostjo in pametnimi mesti, je treba upoštevati ne samo potenciale različnih tehnologij in rešitev, temveč tudi potrebe in dileme, ki se pojavijo sočasno s tehnološkim razvojem, primarno na področju razvoja kadrovskih kompetenc in prilagoditve normativnih okvirjev. Pregled literature pokaže, da obstajajo redke znanstvene objave, ki multidimenzionalno proučujejo simbiozo pametnih mest in policijske dejavnosti. Prispevek zato dopolnjuje obstoječa dela in znanja na tem področju.

UDK: 351.78:004.7

Ključne besede: pametna mesta, zagotavljanje varnosti, policijska dejavnost, kriminalistično preiskovanje, kriminalističnoobveščevalna dejavnost

1 INTRODUCTION

Technological development undoubtedly had and continues to have such an immense impact on human lives that modern societies are developing with evolutionary dynamics. According to Ramaprasad, Sánchez-Ortiz and Syn (2017), the technological development of societies also led to the transformation of cities. In the earliest days, human beings lived in groups since they improved the chances of their survival. The settlements that developed from this coherent style of living led to the development of urbane environments. It is today estimated that 55% of the world's population lives in urban settlements. By 2030, urban areas are projected to house 68% of people globally (United Nations, 2018). In Europe, for instance, "urban areas are home to over two-thirds of the EU's population, and they account for about 80% of energy use and generate up to 85% of Europe's GDP" (European Commission, n. d. b). The first settlements formed in response to certain challenges (i.e. dangers arising from the natural elements, animals and/or dangerous groups). Yet, the growing number of people demanding miscellaneous infrastructure, in a social and physical sense, led to the creation of complex cities, where "the rapid urban growth that brings traffic congestion, pollution, and increasing social inequality may turn the city into a point of convergence of many risks (economic, demographic, social, and environmental)" (Ramaprasad et al., 2017, pp. 13–14). In a way, the city itself is becoming a threat to human beings, entailing the culmination of different threats, among which physical and social threats dominate. Physical threats come from traffic, malfunctioning infrastructure (damaged power lines, collapsing buildings, fires etc.), poor air, water etc. quality, or the occurrence of transmittable diseases. 'Social' dangers are reflected in criminality, and they usually grow with the size of a city. With population growth crimes and criminals are becoming more sophisticated (FICCI-E&Y, 2015). In recent years, new and complex threats have emerged, highlighting the need for closer and more efficient cooperation at all levels. Terrorism, organised crime and cybercrime are today considered the top modern threats and defined as priorities by the European Commission (2015) in its European Agenda on Security.

Nevertheless, cities have a rising number of tools available to combat these problems and acts of crime, where modern technology is one of them (The

Economist Intelligence Unit, 2017). Therefore, we can see cities as both a source *of* and *a solution to* today's economic, environmental and social challenges. By integrating modern information and communications technology [ICT] into cities' infrastructure, we can support their development, management and overall governance. Modern ICT can be used to address various issues and problems related to living and working in urban cities, including security and feelings of safety. A 'smart city' refers to the situation when a city's operations and basic functions are supported by smart solutions and modern ICT. Accordingly, global market trends show significant growth in user demands and investments in so-called smart security solutions. In several developed countries, security stakeholders' awareness has also increased and thus (public and private) security organisations are already adapting to these trends and employing new technologies to improve their responsiveness, legitimacy and overall efficiency. The vision of smart security, which is a sub-system of a smart city, is to help address common security problems and, above all, contribute to the more efficient operations of security organisations.

Two main trends encourage the development of smart security solutions:

- The de-etatisation and decentralisation of security responsibilities and policing activities, which includes plural policing (Modic, Lobnikar, & Dvojmoč, 2014; Sotlar, 2015),[1] the segregation of duties between different public and private, national and local security stakeholders, which in turn requires a multi-stakeholder approach to ensuring safety and security (Boels & Verhage, 2016; Sotlar, 2015). This leads to a stronger need for improved coordination, information management, data sharing and communication systems.
- The evolution of security risks, which refers to the fact that security threats and events are becoming more unpredictable, organised and hybrid, making them more unpredictable and harder to manage (European Commission, 2016). This stimulates a stakeholders' consideration of the potential of modern ICT, and higher investments in research and development, especially smart detection solutions.[2]

Yet while smart city technologies can bring substantial advances to the overall quality of life, they also (by)produce a substantial quantity of data (i.e. big data)[3]

1 *The main challenge of plural policing relates to co-operation between the various organisations. Intra-city traffic violations, maintaining public law and order in the cities and similar tasks are for example more and more performed by municipal wardens. However, the most serious offences and crime-related issues certainly continue to be a task for the police and other law enforcement agencies [LEAs].*

2 *Market growth (the CAGR approximately 10%) of the security industry is predicted to stay stable, which is related to the rising popularity of smart security products (Grand View Research, 2018; Stratistics Market Research Consulting, 2017). The global market in physical security is expected to grow by 100% between 2017 and 2023 (Allied Market Research, 2018).*

3 *Završnik (2018a) states that we can speak of big data if six characteristics are present, namely: I) there is big volume of data; II) data is processed very quickly; III) there is a high variety of data; IV) there is a strong veracity of data; V) the value of the data is high; and VI) there is a certain vulnerability of such data.*

that can be used either positively (predictive analyses, scientific research etc.)[4] or negatively, where the most noticeable are privacy violations (Galdon-Clavell, 2013; Talari et al., 2017; van Zoonen, 2016). This paper addresses some of these concerns, with a specific look at the use of different SCTS and the data of smart cities for police and criminal investigative work. The purpose of the paper is to introduce the relationship of two trending topics which are developing alongside each other but are often separately researched. The possible symbiosis of these two concepts – policing and smart cities – is presented, together with use cases and global forecasts.

The paper may be useful for national and local security organisations and other users wishing to monitor global trends in the area of policing smart cities. It is particularly relevant for the shareholders operating in the security domain seeking to become actively involved in its development. The paper is structured as follows: the first section introduces the concepts of smart city, the second provides a more detailed description of the smart cities concept, the third considers the connection between smart technologies and policing, with subchapters more narrowly focusing on the symbiosis between smart cities, criminal intelligence and criminal investigation. The fourth section discusses privacy concerns in relation to SCTS. The last, fifth section summarises the findings and discusses a set of issues in need of research to support further discussion on the issues of usability and matters of smart cities.

2 SMART CITIES

Smart cities (also known as cyberville, digital city, electronic community, flexicity, information city, intelligent city, knowledge-based city, MESH city, telecity, teletopia, ubiquitous city, wired city; (Eremia, Toma, & Sanduleac, 2017; Komninos, 2008)) are a relatively new concept and thus no standard definition has been developed yet, although varying explanations and interpretations are available:

- A smart city is a place where traditional networks and services are made more efficient with the use of digital and telecommunication technologies for the benefit of its inhabitants and business. (European Commission, n. d. a)
- A smart city uses information and communication technology to enhance its livability, workability and sustainability. It collects information about itself using sensors, devices or other systems, and sends the data to an analytics system to understand what's happening now and what's likely to happen next. (Berst & Logsdon, 2016)
- A place where traditional networks and services are made more flexible, efficient, and sustainable with the use of information, digital

4 *Since the amount of data is so vast and diverse, big data is in a way a "theories generator" and not only an empirical pool used for theory testing (Završnik, 2018b). This implies the natural usefulness of big data for a grounded theory methodological approach (Glaser & Strauss, 2009). Frequently connected to smart cities is the so-called living lab 'approach' where research projects use the city sensors and the (big) data they accumulate to research various aspects of human behaviour. There are numerous such labs (for a list, see The European Network of Living Labs (ENoLL), n. d.), although the such use of city sensors and their data is not to be considered as being without dangers (Galič, 2018).*

and telecommunication technologies, to improve [city'] operations for the benefit of its inhabitants. Smart cities are greener, safer, faster and friendlier. (Mohanty, Choppali, & Kougianos, 2016, p. 60)

- 'Smart cities' is a term denoting the effective integration of physical, digital and human systems in the built environment to deliver sustainable, prosperous and inclusive future for its citizens. (The British Standards Institution, 2014, p. 3)
- A smart city uses digital technology to connect, protect, and enhance the lives of citizens. IoT (Internet of Things) sensors, video cameras, social media, and other inputs act as a nervous system, providing the city operator and citizens with constant feedback so they can make informed decisions. (CISCO, n. d.)
- There is no doubt that a Smart City is a multidisciplinary concept that embodies not only its information technology infrastructure but also its capacity to manage the information and resources to improve the quality of lives of its people. (Ramaprasad et al., 2017, p. 15)
- … an intelligent city is a multi-layer territorial system of innovation. It brings together knowledge-intensive activities, cooperation-based institutions for distributed problem-solving, and digital communication spaces to maximise this problem solving capability. (Komninos, 2008, pp. 123–124)
- Smart cities are an endeavour to make cities more efficient, sustainable and liveable. In other words, a smart city is a city that can monitor and integrate functionality of all the critical infrastructure like roads, tunnels, airways, waterways, railways, communication power supply, etc., control maintenance activities and can help in optimizing the resources while keeping an eye on the security issues as well. (Joshi, Saxena, Godbole, & Shreya, 2016, p. 902)

The common theme of these smart city interpretations is the use of ICT and other technologies to improve public services in combination with personnel and innovative developers. Since this approach generates a substantial amount of data (Mohammadi & Al-Fuqaha, 2018; Mohanty et al., 2016; van Zoonen, 2016; Završnik, 2018b), it influences the relationship between residents, data and governance (Powell, 2014).

We propose a summary definition that encompasses the notions listed above and thus, in our view, smart cities can generally be described as complex ecosystems and living organisms that are aware and constantly evolving. They may be seen as a learning places that, with the help of modern technology, collect and analyse various data, and adapt their services to the needs of the community and their problems. The smart city ecosystem has three main pillars: People/ Technology/Skills and competencies.

The purpose of merging these elements is to create synergy in the form of innovations that solve the problems of a certain community. The main goal is to develop products or solutions that help improve the quality of services, reduce current costs and negative environmental impacts, and increase the public sector's response to solving communities' problems.

Among the several characteristics that define a smart city (Eremia et al., 2017), one of the main ones often stressed in existing smart city frameworks is its multidimensionality. Often referred to, the Giffinger et al. (2007) model describes six pillars of smart cities:

- Smart economy: improving the local economy's competitiveness through innovation and entrepreneurship;
- Smart environment: greater energy efficiency, a green economy, sustainable resource management;
- Smart governance: digitisation of public administration and open data;
- Smart living: improved quality of life supported by technology and advanced solutions in the fields of health, safety and culture;
- Smart mobility: better logistics in transport and traffic management;
- Smart people: incentives with the aim of developing new skills, improving competences, creativity, level of qualification and participation of people in public life (also see Joshi et al., 2016).

Considering the diversity of smart city sub-systems, it is crucial for the various stakeholders, primarily residents, to be involved as a source of information in the development process. Here, we mean a co-innovation process with reference to the triple helix approach, which states that, in addition to the public, three core groups of stakeholders should be involved: policymakers, researchers and industry that can, by sharing views and ideas, achieve real synergy (Leydesdorff & Deakin, 2011).

Smart technologies have many purposes and possible applications. One of the smart city's sub-systems is a safe city supported by smart security that covers all safety aspects of the city. A safe city in a smart city is a city that by integrating technology into the natural environment increases the effectiveness of safety-related processes in order to reduce crime and terror threats, to allow its citizens to live in a healthy environment, have simple access to healthcare, and achieve readiness to be able to quickly respond to threatening emergencies (Lacinák & Ristvej, 2017). Here the question appears of how the policing of smart cities should be organised and how these two systems can mutually benefit each other.

3 SMART CITIES AND THEIR POLICING IMPLICATIONS

Apart from the mentioned trend of plural policing, authors (e.g. Newburn, 2007; Willis, 2014) also note that while reactive and routine-based policing remains the principal policing style, there is a great demand to change the style of policing to become more proactively focused (Newburn, 2007). Consequently, policing styles are emerging that rely on analytical and/or data driven, informed policing related decision-making. Most prominent are evidence-based policing [EB], intelligence-led policing [ILP] (Ratcliffe, 2008), problem-oriented policing [POP] (Braga, 2014) and the type most affected by smart and innovative technologies – predictive policing [PP] (Završnik, 2018b). While all forms of policing take

advantage of advances in ICT (SeaSkate, 1998) and policing research,[5] PP is the type that utilises it the most. By using computerised analysis of mass data on past crime, local environment, temperature and other seemingly unimportant information, state security entities can predict and prevent crime or improve LEAs' responses since predictive algorithms can indicate where they will be possibly needed. It should also be noted that prediction methods are not sufficient for the arrest of a suspect because the predictions are generated by statistical processing as part of the analysis of past criminal data and other data. They only produce rough estimates and probabilities of events in the future so this information must be considered as merely giving support for other more traditional policework forms (Perry, McInnis, Price, Smith, & Hollywood, 2013). Such use of ICT for safety and security reasons has triggered discussion of the implications of big data analysis for policing and crime preventions. Despite the undeniable potential held by big data for such purposes, certain core issues remain:

- the data are actually subjective (the data are among other sources generated from police statistics that are racially biased) (Završnik, 2018b); and
- big data is extensive, thereby bringing with it the issues of proper analytics and data management (Baig et al., 2017; Mohammadi & Al-Fuqaha, 2018).

However, while its applicability must still be tested for these two core issues, examples of the application of PP in Chicago[6] (Douglas, 2018) or Santa Cruz (California)[7] (Rich, 2011) are seen as promising.

Data for police use may be generated by using digitised records of criminals, CCTV, unmanned (aerial, (under)water, ground) vehicles, body-worn cameras, social media feeds and data analytics,[8] application of Artificial Intelligence

5 *Nowadays, ICT is used in almost every aspect of police work. From dispatch calls, patrol tracking and for communicating to various improvements in crime scene investigations, to report writing and analysing (SeaSkate, 1998).*

6 *As Douglas (2018) writes "…//using the latest in IT, including video surveillance and computer analysis of incidents, is reducing violent crime in the city". With regard to statistics "Citywide, shootings dropped 21 percent in 2017 compared to 2016, … //… and in districts No. 7 and 11, on the city's southern and western sides — home to the first two [Strategic Decision Support Centers] — shootings are down 33 percent."*

7 *The pilot project can be described as successful. Software uses specially designed algorithms to calculate and predict crime hotspots and then suggest where police patrolling should take place. "In the nearly two months of use, the pilot has garnered positive results. Since the pilot's deployment, the model has correctly predicted 40 percent of the crimes that it was aiming to predict, and the Santa Cruz Police Department has seen a reduction in the types of crime that it's been addressing. In addition, the Police Department saw a 27 percent decrease in the number of reported burglaries in July compared with July 2010." (Rich, 2011)*

8 *A report by FICCIJA and Ernst&Young (FICCI-E&Y, 2015, p. 16) gives an example of the Los Angeles Police Department's (LAPD) usage of "social media to help guide department operations during major events such as the NBA All Star Game in 2011 and the Stanley Cup playoffs in 2012. During these events, the department tracked large-scale parties and other gatherings throughout the city, and deployed teams of building inspectors, police officers, and fire department officials to ensure the events were legal and safe. The department also monitored social media to keep a tab on 'trending' topics, such as whether large crowds of people planned to head downtown, and adjusted deployment plans accordingly. The LAPD has fully integrated its social media branch into the command post structure for major events. The social media branch is responsible for briefing the incident commander about relevant activities on social media."*

[AI] etc. as well as via the traditional police officer–citizen relationship.[9] Police departments create large volumes of digitised data which may improve officers' decision-making (FICCI-E&Y, 2015). In essence, this relationship between smart cities and ICT technology in policing would entail so-called smart policing. Smart policing may be defined by the use of modern technology and processes that increases police officers' efficiency and effectiveness in the field. It should include real-time data, social media communication, field tablets, predictive policing tools, and several other options (FICCI-E&Y, 2015).

While smart technology is presently used to prevent and/or to react to (respond, sanitise, investigate) an incident deriving from human behaviour, the latest trend is moving strongly in the direction of attempts to modify human behaviour. One example is China's Social Credit System that ranks residents (they 'collect' or 'lose' points) for their adherence to (in)formal social rules and their overall diligence (paying bills on time, committing traffic violations etc.) (Larson, 2018). This may be seen as an extreme form of (Pavlov) conditioning where technology plays the role of a stringent ever-present watchman. In line with routine activity theory, such technology for monitoring can deter crime since the third factor (the absence of a capable guardian) does not apply – the guardian is 'always' present. Going a step further, social media – an important part of the smart city by connecting the city with its inhabitants – is a tool of unprecedented usability. There are indications that, for example, voting behaviour and actual candidate choices have been affected by such (ab)use of social media (Završnik, 2018a). Undoubtedly, this holds substantial implications for the threat landscape and thus for policing. The questions regarding smart cities and policing have focused primarily on the increased surveillance capacity a highly networked urban setting provides for law enforcement. SCTS can trigger the response of criminal investigative apparatus with the proactive or real-time detection of criminal acts and security incidents.

3.1 (Criminal) Investigation and smart cities

Criminal investigation can be defined as "the process of discovering, collecting, preparing, identifying and presenting evidence to determine what happened and who is responsible" (Hess & Orthmann, 2010, p. 6). Palmiotto (2013, p. 4) explains "[C]riminal investigation is a thinking and reasoning process. The modern investigator's primary objective is to gather facts about a criminal situation. This objective is accomplished by collecting all the accurate information pertaining to a specific act or crime". In essence, this usually pertains to an array of activities – depending on the form of the criminal justice system – by the police, prosecutors and judicial branch (Maver et al., 2004). A criminal investigation typically starts upon the discovery of an event or its consequences that have signs of a crime. It is not always necessary that an investigation will confirm a crime was conducted

9 *In a more critical view, the option that citizens with their smart devices report acts of deviant behaviours to the police is what Završnik, (2018a, p. 48) denotes as "community policing 3.0", marking citizens as "walking sensors" and an actual part of the smart grid sensor system.*

(Dvoršek, 2008); therefore, some authors (e.g. Bryant, 2010) contend the main goal of a criminal investigation is to know the *truth*. A crucial element in explaining the subject events is information (Gottschalk, 2010) and other data upon which criminal investigators can build while reconstructing the timeline causality of events. That is why it is perhaps easy to see criminal investigations as a reactive activity. However, they can also be proactive when investigators with informational analytics, criminal intelligence[10] or informants and other sources predict criminal behaviours. This short definitional narrative shows that *information* is absolutely crucial for an effective criminal investigation. This is also the core reason we can assert that there is a natural symbiosis of smart cities, criminal investigations and/or criminal intelligence.

3.2 The Benefits of SCTS for Criminal Investigation and Intelligence

While gunshot,[11] scream or glass-shattering sensors, traffic accidents alert systems etc. are chiefly used to expedite faster responses from first-line responders, they can also be used in criminal investigations. Some examples are given in the following use cases.

The log files of sensors give very precise information for specifying the time of an event. This information is probably far more accurate than eyewitness accounts. Log data generated by smart vehicles that 'communicate' with smart city infrastructure in order to give drivers and passengers the most up-to-date information on one hand or to adjust city traffic systems on the other (Baig et al., 2017) can in criminal investigations be retrieved from either the vehicles or the city system and used to establish alibis, traveling routes etc.

Weather-monitoring systems data can be used to more easily or more properly interpret crime scene traces. Environmental factors and the weather situation must always be documented at crime scenes (Maver et al., 2004; Palmiotto, 2013) and later considered in the investigation (e.g. air temperature, precipitation data can be used to more accurately determine the time of death; wind speed and direction can be used for ballistic reconstructions etc.).

Smart cities (or neighbourhoods) also use Wi-Fi systems to first provide free Internet access and/or provide information to those entering a certain area. This, in turn, means data are created concerning mobile phones that have entered a particular space (Galič, 2018). Such data can be used in criminal investigations when we are interested in the movement of a given person, or when a certain timeline must be established. It can also be used to transmit crucial information such as Amber alerts or information on missing or wanted persons.

One may presume that the good sensor grid systems established and utilised for monitoring air or water quality (Talari et al., 2017) could detect illegal waste

10 *Ratcliffe (2008, p. 7) uses the term crime intelligence in his book »as a collective term to describe the result of the analysis of not only covert information from surveillance, offender interviews and confidential human sources (informants), but also crime patterns and police data sources as well as socio-demographic data and other non-police data«.*

11 *Gunshot sensors are acoustic sensors that can be used to detect firearms use and localise the shooter (Khalid, Babar, Zafar, & Zuhairi, 2013).*

dumping. Similarly, smart meters for electric consumption that ease the reporting of electricity consumption to the supplier (Galdon-Clavell, 2013) could also be used to identify possible locations for indoor growing of cannabis (Baig et al., 2017).

Platforms that enable citizens to submit initiatives to improve the quality of life in a city or to report issues they encounter in their lives could also be used as portals for reporting and helping to discover crimes. Such communication with a citizen, usually via social media, is recognised as critical tool for smart cities (Joshi et al., 2016) and thus also useful for various policing tasks. The accumulated data from platforms that allow citizens to submit initiatives for improving the quality of life in the city or to report issues they encounter in their lives is a basis for criminal intelligence to more efficiently build its analytical and intelligence products. This, in turn, can be used to detect emerging crime issues and trends or to influence decision-makers to adapt/change the policing style in a certain area.

In cases of tactical intelligence, namely, where intelligence is used for a specific event (Peterson, 2005), data from SCTS can also be relied on. Pereira, Macadar, Luciano and Testa (2017) in a paper for which they interviewed several personnel working with(in) the Centre of Operations Rio de Janeiro (a form of smart city control and analytics centre) report how good cooperation between the developers of a traffic application and the city administration facilitated better work and overall handling of the situations during the Pope's visit to Brazil.

Citizen participation (e.g. crowdsourcing) platforms in a way also enable citizens to become more empowered and included in the city governance, especially if platforms also include feedback from the city leadership or an agency to which a comment or criticism was intended. Such communication channels, if effective, can reduce dissatisfaction with the city or public administration (Pereira et al., 2017). This could thereby also be a form of crime prevention since communicational feedback gives a person the feeling of having been heard and in some cases prevents negative attention seeking/retributive behaviour (e.g. sending envelopes with white dust to administration offices, threats to public officials etc.).

3.3 The Benefit of Criminal Intelligence and/or Criminal Investigations for Smart Cities

In contrast to the criminal intelligence contribution to smart city systems, due to their focus and the specificity of an individual event, criminal investigations inputs are somewhat limited. The greatest benefit is observed when a smart city system infrastructure is under attack or a crime has been committed against the city itself (e.g. intrusions in various systems that run city power lines, traffic systems etc.) and where digital forensics is used to investigate the event. The data derived from such investigations represent a form of system vulnerability test and can be used to improve the security of the mentioned systems (Baig et al., 2017).

On the other side, strategic intelligence, which deals with information with regard to crime trends and among others develops crime-control strategies (Peterson, 2005), can be used to pinpoint the locations where SCTS can/should be applied. Alternatively, to determine what sort of technology is needed to tackle a

given form of crime in a specific area, e.g. smart lights and aroma diffusers can be used in a particular area at a defined time. The selection of the area, time and form of technology can be based on crime statistics, criminology scholarship as well as a range of other data (mobile phone data, social media analysis etc.) (Meijer & Thaens, 2018). This implies that 'smart' technology is an element of situational prevention.

The broad array of the underlying relationship between smart cities and different policing forms is summarised in Figure 1 below.

Figure 1: Graphic illustration of relationships between smart cities, policing, criminal intelligence and criminal investigations

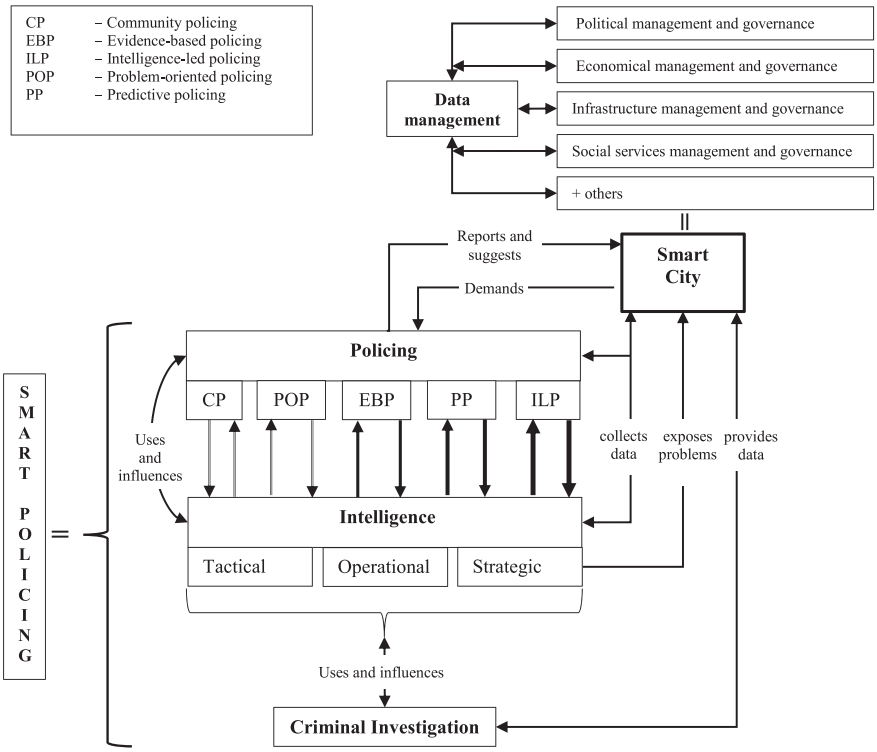

Figure 1 shows a model of correlations between smart cities, policing, criminal intelligence and criminal investigation. Technologies that support smart city functions enable more effective and efficient data management in governing political, economic, infrastructure and social divisions. The information produced by smart cities is usable in all areas related to public security provision, and also for different types of policing. The model also reflects that smart city data management can support the development of smart policing.

While the above figure shows the relationship between different actors and functions that (or at least should) work together to provide security, the technologies that (could) provide data and support policing activities take many different forms. Table 1 below summarises some of the most common core smart city technologies and their possible use for policing, criminal intelligence and criminal investigations.

Table 1: Technology used in smart cities and most easily used in policing, criminal intelligence and criminal investigations

Technology/ system	Primary use	Potential for policing	Potential for Criminal Investigations and/or Criminal Intelligence*
4G / 5G networks	Broadband mobile communications (cellular wireless networks) with high speed, reliability and coverage.	Improved data communications between officer(s), control centres, patrols etc. Networks that enable more (not just voice) and better data to be communicated.	Such networks that enable data (voice, imagery, diagnostics etc.) from various personnel to be recorded or transferred. This in turn eases investigators' work by providing data (evidence) for their cases or real-time information search. If the data recorded or transferred via such networks is analysed more coherently, it can be used for strategic, tactical or operational intelligence, e.g. data mining.
Body-worn cameras and devices	Provide a feed from human operators to control/support centres to obtain information on the psychological or psychical status of the operators, to give support staff enough data to provide support to operators, provide imagery for further analysis (used by army, astronauts, police, in a way also surgeons, divers etc.).	Wearing body cameras by patrolling police officers influences their own behaviour and of persons in police procedures.	Imagery from police officers' body cameras provide data for criminal investigations and can also give evidence of use in investigations. If data is analysed in a more coherent way it can be used for tactical or operational intelligence (can provide info on suspects and locations for breaching actions).
Advanced CCTV	Active video surveillance of locations connected to monitoring systems that include recognition and alarm capabilities and retrospective analytics.	Monitoring locations, events and disruption identification. For example, detecting potentially malicious behaviour, followed by further real-time, pro-active investigative techniques.	Gathering and reviewing information for a specific location/event/ person(s). Can provide evidence useful for investigating crimes already committed. Such technology can from the point of criminal intelligence be used for targeted monitoring of persons of interest. It also has the potential for tactical or operational intelligence.
Geographic information systems (GIS)	Various analytical, research and diagnostic usage. Pollution, traffic, geological etc. monitoring.	Mapping of crime 'hot spots'.	Provides data/information to criminal investigators and/or assists with the development of timelines, mapping locations of crucial events. If data is analysed more coherently, it can be used for strategic planning or tactical and operational intelligence, e.g. suspect movement analysis etc.

Table 1: Continuation

Technology/ system	Primary use	Potential for policing	Potential for Criminal Investigations and/or Criminal Intelligence*
IoT	Collection and storage of various data. Connectivity among devices enables better usability, monitoring, controlling and diagnostics of devices connected with each other (long-distance management of electronic grids, reduced electricity consumption etc.).	Crime analytics, predictive policing, crime mapping.	Provides data that can be used in investigations (e.g. electricity consumption and illegal laboratories). The IoT promises extreme usefulness for criminal intelligence – in a strategic, operational and tactical sense, e.g. building a portfolio of places, people and behaviours – used to plan proper actions or responses.
Sound sensors for screams or gunshots or breaking glass	To activate first responders or automatically notify security personnel in the near proximity that an incident might be developing.	Faster detection of events and lower police response time.	Data logs from such a sensor provide precise information as to when a specific sound was detected – helping to establish an event timeline. If data is analysed in a more coherent way, it can be used for strategic, tactical or operational intelligence, e.g. analysing criminal behaviour patterns at a certain location.
Smart public lightning system	Improved management and effectiveness of the public lighting system and sensors installed on light posts can all be used for monitoring traffic, pollution etc. levels.	Adapting the brightness level to various situations influences crime prevention or officer safety (e.g. brightening to provide greater security or an overview of some location).	Crime scenes can be better examined at night if the brightness can be adjusted, sensors on light posts can provide data for crime investigations.
Smart grids (of any kind)	Provide a better user experience and easier control of the matter (electricity, water, gas, Internet, traffic etc.) transmitted in the grid. Smart grids could also be used for research and predictive analysis. E.g. smart electricity consumption monitoring technology could be used for other purposes such as determining the size of the informal economy by monitoring electricity consumption.	Some grids (traffic-related) provide more safety than non-smart grids. For example, the usage of AI makes traffic flows more fluid.	Crimes can be more easily detected. Some data generated from the smart grid log systems can be used in investigations. If data is analysed more coherently, it can be used for tactical or operational intelligence, e.g. detecting criminal behaviour related to consumption of what is transmitted through the grid.

Table 1: Continuation

Technology/ system	Primary use	Potential for policing	Potential for Criminal Investigations and/or Criminal Intelligence*
Social media monitoring tools and crowdsourcing platforms	Gathering intelligence with advanced analytics performed on social media content, gathering information from the public.	Planning activities, detecting societal problems, public communication.	Social media contributions by suspects, witnesses or other sources can be useful for investigators as they can post information about a particular event, person or location. Such data can be used as evidence in proper circumstances. Gathering data from user posts and communication on events, locations and people monitoring. As part of OSINT, the value is diverse.
Unmanned aerial vehicles ('drones')	Various monitoring of situations and scanning locations or objects (geographical scanning, aerial photography); delivery of products; general consumerism (hobby, DIY development etc.); multimedia (movie making) and more.	Monitoring of events, locations and people.	Crime scene investigations (aerial photography), covert surveillance etc. If data is analysed in a more coherent way, it can be used for strategic, tactical or operational intelligence. Analysing criminal behaviour, gathering intel for breaching actions or high-profile arrests etc.

* Since police investigators use products of criminal intelligence, the primary users and in fact the form of technology use cannot be always clearly abstracted, we therefore jointly provide examples for criminal intelligence and criminal investigation use of the most common technologies. The Criminal Intelligence segments build heavily on the work of Peterson (2005).

4 PRIVACY CONCERNS

As indicated, smart cities amass enormous volumes of data and the opening up of this data for application creates different, legitimate privacy concerns (Galdon-Clavell, 2013; Galič, 2018; Kanduč, 2018; Talari et al., 2017; van Zoonen, 2016; Završnik, 2018b). As Fujs and Markelj (2018) observed, smart technologies give people a certain degree of leisure in return for lower privacy. The concern is not just that the government will utilise the technology to spy on people, but the technologies and data can also be hacked by criminals (Baig et al., 2017) for use in an array of criminal acts or misused by businesses (Galič, 2018; Kanduč, 2018; Završnik, 2018a). The latter might occur intentionally or unintentionally as the mishap of Amazon's Echo system revealed when the system erroneously recorded and made private conversations public (Chokshi, 2018).[12] Although

12 *Due to the sheer number of these systems sold and installed and the manner of how they work and what they do – the system hibernates and waits for speech commands from the users, when commands are given, they are recorded and executed by the system. In turn, systems store a variety of data (speech recordings, usage logs, device cache as well as other data such as calendars or to-do list) on the Amazon cloud service and/or devices themselves. This data promises great usability for criminal investigations (Orr & Sanchez, 2018), either from the point of criminal intelligence where investigators can gather data on a person of interest or perhaps even use these systems for undercover surveillance. In less intrusive purposes, criminal investigators can use data for establishing timelines, alibies etc.*

people are willing to accept constant monitoring and are self-motivated to share their private data with private businesses in order to obtain better services or some loyalty points and discounts (for example, numerous loyalty clubs, cards and lists promise different benefits in return for data on our purchase, viewing, communicating, driving, sleeping, recreating etc. habits), they also lawfully, albeit naively, expect the information will not be compromised or misused. In democratic countries scoring high on the human freedom index, people often see these rights as self-evident and generally take them for granted – customer expectations arise from given regulatory safeguards and beliefs that the system works, and that organisations are properly monitored. However, in reality, when using different services and applications people's privacy depends strongly on the integrity and ethics of (service) providers since users have a very limited insight into the security and protection of the data, while how effective control mechanisms are depends on various factors (customers' reports, staff workload, varying regulations in different states etc). Nevertheless, the new Regulation (EU) 2016/679 of the European Parliament and of the Council (2016) (EU General Data Protection Regulation [GDPR]) recently implemented across the EU looks promising and might also encourage the greater social responsibility of service providers and data collectors. Thus, concerns remain that everyday elements that are carried/worn (smartphones, smartwatches, and accessories, NFC key rings, wallets, even clothes) that have built-in systems or chips (NFC, RFID tags etc.) will be turned into a targeted person-monitoring tool. The same concerns also relate to the use of SCTS. For example, there is a perceived danger that LEAs could utilise the smart city grid of sensors to track and monitor individuals. Consideration and caution are clearly necessary, yet if there is a sufficient burden of proof or if an intelligence agency does not need one it is far simpler to just directly install Trojan-type software on a suspect's electronic device (Abel, 2009) or wearable accessory and use that to track and monitor them, without relying on the smart city grid of sensors.[13] In any case, the proper regulative framework must be developed and enforced to prevent unlawful access to and distribution of data generated by SCTS. By this, we refer mainly to the legal loopholes which are very common due to fast pace of technological development. Spencer (2017), for example, points to the framework in the United States of America which, for instance, states that while privacy (and thereby data) against unlawful searches is protected by Fourth Amendment, this protection does not apply to third parties. This means that data is only protected from LEAs and not from businesses, which could be (ab)used by LEAs to 'outsource' data gathering.

Van Zoonen (2016) notes that discussions of privacy concerns in connection with smart cities should consider types of data, the purpose of the data, and their collectors. There is a complex diversity of factors influencing levels of risk for privacy violations. In our view, the risk level depends on the combination of three factors connected to data generated by SCTS. Namely: 1) users (*who uses the data?*); 2) purposes (*for what is the data being used?*) and 3) form (*what sorts of data?*):

13 *For example, several media reported that Germany's Federal Criminal Police Office (BKA) is using a Trojan virus as a tool to access data of suspected individuals on their smartphones before the information becomes encrypted by apps such as Telegram and WhatsApp (Burack, 2018).*

1. Users (*who*): While studies show that big data promise great positive usability for improving the quality of citizens' lives (Pereira et al., 2017), there is a difference if such data is analysed by an LEA or an agency whose task does not include potential prosecution. Actors operating with data generated for and/or by SCTS can be divided into three groups: the civil sphere (developers and maintainers of SCTS); the plural policing sphere (municipality wardens, private security); and the LEA sphere (police, certain intelligence agencies etc.). Of course, a certain liaison line can be established between them, e.g. when electricity suppliers use smart grids to monitor the residents' electricity consumption and then report anomalies to the LEA. Depending on the protocol that dictates how to screen the grid for such anomalies and how (under which level of suspicion should the electricity supplier report/alert the LEA or how often), the risk for privacy violations can also be diverse.
2. Purposes (*why*). Considering the above-mentioned wide list of actors, the data may have a range of uses. While the civil sphere will use data generated by SCTS to maintain the smart city and its further development, the actors of plural policing can use data for maintaining public law and order, improving the quality of their services etc. Actors from the LEA could take advantage of the data for strategic criminal intelligence (crime prevention aims) or specific criminal investigative purposes (investigation of a particular crime and prosecution of a certain person(s)).
3. Form (*what sorts of data*): We have recognised three different sets of data, namely: 1) "raw" data from diagnostic logs of systems (runtime, auto diagnostic, system checks, system incidents diagnostics etc.) – this data does not hold strong individualisation and identification markers; 2) mass data from sensors (vehicle licence plates in a certain area, phone/tablet data used to communicate with a system etc.) – data is individualised yet additional data is needed to properly identify a subject (e.g. you need access to the database of vehicle registration information to identify a vehicle's owner, but you still do not know who actually drove that vehicle to that location at that time); and 3) strongly individualised data (biometric data, data from fingerprint locks, photographs and other visual data etc.). All three data categories demand different sharing rights and safeguards. For instance, data from the first category are not a threat to privacy since they are not connected to persons or individuals and can thus be undisputedly used by SCTS developers and maintenance teams in their daily work, while the same data could be provided to the LEA, but only in connection with a specific investigation or for crime-prevention measures (here special contracts between data providers and LEAs must be established in advance and detail how data must be protected and how it may be used). Data from the second and third categories should be provided to the LEA only upon judicial demand. If the LEA is the one gathering data, a special access protocol must be developed that tracks who, when and why the

data was accessed. Analysis of these data for other purposes is possible as well, but they must be anonymised to exempt them from personal data confidentiality and privacy related restrictions.

A mix of the aforementioned narratives (who, why and what) influences the emergence of different levels of risk for privacy violations. It may be considered that the risk of privacy violations is low if SCTS maintenance teams use depersonalised diagnostic data logs. In contrast, with strongly individualised data, for instance CCTV recordings used by LEA to monitor person(s) behaviours, the risk for privacy violations can be high (for a similar discussion, see van Zoonen, 2016). Ensuring the proper security and management of the data used and/or generated by smart city systems is therefore essential (Talari et al., 2017), which is why information and cyber security and defence, together with proper compliance and usage monitoring represent crucial safeguards. Numerous standards pertain to smart cities or their component parts and can help governments, cities or developers address various issues. While standards such as UNE 178301:2015, PNE 178106, PNE 178306, PNE 178501, PAS 182 and 183 etc. assure the proper development of smart city infrastructure, SCTS and data management, more comprehensive models and standards are also available and useful for managing and planning smart cities' development, such as PAS 181, PD 8101 ISO/TS 37151:2015, ISO 37120:2014, ISO/DIS 37101, ISO/DTR 37121, ISO/NP 37122, ISO/WD 37120. Further, standards like ISO/IEC 27001: 2013, ISO/IEC 27002: 2013 or IEC 62443 are also very important by including guidelines and measures for the proper development of information and cyber security. Guidelines and legislative frameworks that would more holistically address SCTS and the data deriving from them are still being developed and so we can expect the emergence of new regulations that will concretise access to and sharing of data with LEA alongside precise definitions of who can have access to which dataset, for which purposes and on which conditions.

4 DISCUSSION AND CONCLUSIONS

It is safe to assume that although SCTS raise great concerns over personal privacy, they will still be used in facilitating urban development. Their potentials for improving the quality of life, the economy and the environment are far too promising, which is why smart cities have become a solution framework recognised on the international level and an objective of many national strategies. When smart cities use systems and technology that do not track individuals, then such smart cities are far from the Orwellian dystopia with which they are so often associated. However, the line between citizen safety provision and citizen monitoring is indeed thin, but this should not discourage us from using such technology and instead encourage us to research and develop it further in the right way.

Smart security connected to the development of safe cities as sub-systems of smart cities is a trending topic in municipal development and governance plans. In this paper, we elaborated on the role of SCTS and their implications

for policing and criminal investigation/intelligence. We emphasised that the data generated by SCTS hold considerable potential for criminal intelligence and/or criminal investigations, yet access to this data should be properly regulated and safeguarded from unlawful LEA (and other agency) usage. In contrast, the products of criminal investigation, but even more so, criminal intelligence analysis could be used to recommend (or even co-develop) SCTS to tackle delinquency or other unwanted behaviour. This symbiosis can be an indicator of smart policing where big data plays a pivotal role in how policing is more effectively conducted.

There is, of course, also a danger that the data generated by SCTS is capitalised by smart city governance ("What truly makes a city intelligent is its capability to innovate and capitalize economically." (Joshi et al., 2016, p. 905)). Here big business, which is exploiting the data so amassed for commercial or even political purposes, is perhaps even a bigger threat to our privacy than police agencies, yet it is rarely seen as such (Galič, 2018; Kanduč, 2018; Završnik, 2018a, 2018b). Moreover, since the development of technologies and systems utilised by smart cities is sometimes made in a public-private partnership, often with private businesses safeguarding the intellectual property rights (Public-private partnerships for SMART city management, 2015), this raises additional concerns with regard to transparency, accountability and privacy.

Since privacy and information security are by far the most relevant issues in the development of smart cities, legitimacy must be considered a key quality of the technologies and solutions that are developed. Here, we must stress the role of people's perceptions of risks and benefits. Perceptions are typically a more crucial factor in adoption and the evaluation of the legitimacy of technologies than their actual design and functions. In practice, this means the pace of smart city development and smart policing depends on perceived risks rather than on their actual state (van Zoonen, 2016). Since the fearing of risks is often irrational, it seems reasonable to also address public opinion and support when promoting such development. For example, people are easily compelled to share their private data, yet are critical of new technologies proposed for LEA use. Steps to further improve the legitimacy of and trust in LEA and public approval of LEAs' use of data derived from ICT and SCTS should focus on improving transparency and promoting the benefits of such usage. Greater transparency could be achieved through better communication about safeguards – citizens must know how data is gathered and used, while the mechanisms the state applies to discover the unlawful behaviour of LEAs (and other agencies) must be promoted, as well as the prosecution of such behaviour. Research by Fujs and Markelj (2018) also shows that public knowledge about smart cities is relatively low and people are concerned with their lack of the technical skills needed to understand and properly use new technologies. That is why publicly-oriented awareness and education programmes must encompass smart city development. At the same time, private entities that provide services that accumulate user data must be compelled to uphold standards and protocols. Periodical political, scientific, non-governmental etc. inquiry into these private entities' behaviour and use of data derived from SCTS should be encouraged and promoted. Clearly, further research into the public perceptions of LEAs' role in the smart city ecosystem is needed. When

discussing possible negative implications of the digitisation and datafication of the city's functions, unease is of course not unreasonable because SCTS generate unprecedented amounts of data that may be used in a variety of ways. They can be exploited by LEAs, private businesses and criminals. Considering that smart cities are the future direction of urban development, it is vital to address the issues concerned with privacy and the development of regulation accordingly. This includes providing proper legislation, guidelines and recommendations or implementing those already developed (Galdon-Clavell, 2013). Proper research must be conducted that dissects the impacts of smart technology, privacy concerns and future development in these spheres (Meijer & Thaens, 2018).[14]

Moreover, we should also encourage setting up some form of watchdog institution/s to safeguard citizen privacy rights and simultaneously monitor the behaviour of governments and businesses. The key question here is whether the current mechanisms and already established institutions (e.g. Information Commissioner) are sufficient for monitoring and preventing privacy violations that are set to become more complex and widespread as smart cities and SCTS develop. In this regard, further discussions and system reviews are needed to clarify whether we need agencies, institutions and watchdogs that would focus exclusively on monitoring the compliance of safe city operations and smart city management, developing regulations and exercising control over advances and the use of SCTS.

At the end of our discussion, there is one other important aspect we need to highlight. In all areas related to the topic of this paper, for example, research and education, public and private sector, there is a growing need for properly educated and competent personnel to deal with smart technologies and related issues. Here students from faculties that provide a combination of ICT knowledge and public administration/governance knowledge would be best qualified. While some countries still perhaps need to develop such study programmes, in Slovenia the Information Security study programme at the Faculty of Criminal Justice and Security of the University of Maribor already produces such a skillset. Further, since students taking this programme also receive knowledge relating to criminal investigation, they are properly equipped to be either users of data produced by smart city technologies (e.g. in the role of criminal investigator or criminal intelligence analyst) or to safeguard against potential privacy intrusion (e.g. if they are in the role of a smart city technology developer or working for a city administration planning to incorporate such technology). In the future, police professionals with insights into ICT as well as criminal investigative know-how will be most appropriately equipped for investigating crimes as their cognitive and critical investigative thinking skills will need to include focusing on the possibilities of data created by ICT or SCTS.

The outcome of this paper calls attention to the knowledge-based approach to managing smart cities. The future success of urban development depends on the awareness, integrity and flexibility of all stakeholders involved. The evolution and transformations of urban life require societies' culture and climate to adapt

14 *We also agree with Baig et al. (2017) that extensive research and developmental focus should be given to the tools and methods of digital forensics that can be used in the IoT, ICT and smart cities.*

to the changes as well. The open-mindedness of citizens and receptiveness of political and governing bodies will play a significant role in the adoption of further innovations. Given market reports and trend predictions (e.g. Deloitte, 2015), the skills and competencies of those responsible will be a major challenge in the provision of effective smart city governance. Recent security incidents around the world (natural disasters, terrorist attacks, mass casualties, use of means of mass destruction, AMOK situations, extortions, organised criminal activities) clearly show the threat landscape is also transforming, while global threats are manifesting in local communities and no society is immune. As a result, security authorities face new situations and risks and often lack specific experience and competencies. Together with the technological development of societies, this problem is only intensifying. The increased complexity of urban communities requires a consideration of professionalising the management of urban safety and security. Thus, challenges relating to the management of urban problems sparked a discussion on the urban security management system. In this relation, the European URBIS project, featuring the Faculty of Criminal Justice and Security as a partner, was carried out to study the professionalisation of urban security managers' role. The essential idea was that the contemporary security environment requires a professional in the community who can meet the whole range of expected challenges. The project reasoned that urban security managers, as coordinators, must possess the skills and knowledge to analyse situations and coordinate a response, enabling them to cooperate successfully with state and local authorities and security provision institutions and organisations, as well as with the general public/society (Meško, Tominc, & Sotlar, 2013). The correlations of smart cities with such observations, by either playing the role of incentives and contributors to problems or as a solution to those problems, is more than evident.

REFERENCES

Abel, W. (2009). Agents, trojans and tags: The next generation of investigators. *International Review of Law, Computers & Technology*, *23*(1–2), 99–108.

Allied Market Research. (2018). *Physical security market by type (system and services), industry vertical (BFSI, commercial, government, residential and transportation) – Global opportunity analysis and industry forecast, 2017–2023*. Retrieved from https://www.alliedmarketresearch.com/physical-security-market

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M. … Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, 3–13.

Berst, J., & Logsdon, D. (October 17, 2016). *The hill: At smart cities week, tackling opportunities and challenges*. Retrieved from https://smartcitiescouncil.com/article/hill-smart-cities-week-tackling-opportunities-and-challenges

Boels, D., & Verhage, A. (2016). Plural policing: A state-of-the-art review. *Policing: An International Journal of Police Strategies & Management*, *39*(1), 2–18.

Braga, A. A. (2014). Problem-oriented policing. In G. Bruinsma, & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. 3989–4000). New York: Springer.

Bryant, R. P. (2010). Theories of criminal investigation. In S. Tong, R. P. Bryant, & M. A. H. Horvath (Eds.), *Understanding criminal investigation* (pp. 13–33). Oxford: Wiley-Blackwell.

Burack, C. (January 27, 2018). German federal police use Trojan virus to evade phone encryption. *Deutsche Welle*. Retreived from https://www.dw.com/en/german-federal-police-use-trojan-virus-to-evade-phone-encryption/a-42328466

Chokshi, N. (May 25, 2018). *Is Alexa listening? Amazon echo sent out recording of couple's conversation*. Retrieved from https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html

CISCO. (n. d.). *What is a smart city?* Retrieved from https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html

Deloitte. (2015). *Smart cities – How rapid advances in technology are reshaping our economy and society* (Version 1.0). The Netherlans: Deloitte. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/public-sector/deloitte-nl-ps-smart-cities-report.pdf

Douglas, T. (January 23, 2018). *Chicago police cut crime with major upgrades to analytics and field technology*. Retrieved from http://www.govtech.com/public-safety/Chicago-Police-Cut-Crime-with-Major-Upgrades-to-Analytics-and-Field-Technology.html

Dvoršek, A. (2008). *Kriminalistična metodika* [Criminal investigative methods]. Ljubljana: Fakulteta za varnostne vede.

Eremia, M., Toma, L., & Sanduleac, M. (2017). The smart city concept in the 21st century. *Procedia Engineering*, *181*, 12–19.

European Commission. (2015). *A European agenda on security (COM/2015/185/FINAL).* Retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

European Commission. (April 6, 2016). *Security: EU strengthens response to hybrid threats*. Retrieved from http://europa.eu/rapid/press-release_IP-16-1227_sl.htm

European Commission. (n. d. a). *Smart cities*. Retrieved from https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en#what-are-smart-cities

European Commission. (n. d. b). *Urban development*. Retrieved from http://ec.europa.eu/regional_policy/en/policy/themes/urban-development/

FICCI-E&Y. (2015). *S.M.A.R.T. policing for smart cities*. Retrieved from http://ficci.in/spdocument/20615/FICCI-Report-SMART-Policing-for-Smart-Cities.pdf

Fujs, D., & Markelj, B. (2018). Privacy in smart cities or privacy for smart people? *Varstvoslovje, 20*(1), 5–24.

Galdon-Clavell, G. (2013). (Not so) smart cities? The drivers, impact and risks of surveillance-enabled smart environments. *Science and Public Policy*, *40*(6), 717–723.

Galič, M. (2018). Živeči laboratoriji in veliko podatkovje v praksi: Stratumseind 2.0 – razprava o živečem laboratoriju na Nizozemskem [Living laboratories and Big Data in practice: Stratumseind 2.0 – debate on a living lab in the Neth-

erlands]. In A. Završnik, & L. Selinšek (Eds.), *Pravo in nadzor v dobi velikega podatkovja* (pp. 85–110). Ljubljana: Pravna fakulteta: Inštitut za kriminologijo pri Pravni fakulteti.

Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanović, N., & Meijers, E. (2007). *Smart cities – ranking of European medium-sized cities*. Vienna: Centre of Regional Science.

Glaser, B. G., & Strauss, A. L. (2009). *The discovery of grounded theory: Strategies for qualitative research*. New Brunswick: Aldine.

Gottschalk, P. (2010). *Policing organized crime: Intelligence strategy implementation*. Boca Raton: CRC Press.

Grand View Research. (2018). *Physical security market worth $290.7 billion by 2025: CAGR: 9.1%*. Retrieved from https://www.grandviewresearch.com/press-release/global-physical-security-market

Hess, K. M., & Orthmann, C. M. H. (2010). *Criminal investigation*. Clifton Park: Delmar, Cengage Learning.

Joshi, S., Saxena, S., Godbole, T., & Shreya. (2016). Developing smart cities: An integrated framework. *Procedia Computer Science*, *93*, 902–909.

Kanduč, Z. (2018). Stroji, podatki, ljudje, kontrola in kapitalizem [Machines, data, people, control and capitalism]. In A. Završnik, & L. Selinšek (Eds.), *Pravo in nadzor v dobi velikega podatkovja* (pp. 133–166). Ljubljana: Pravna fakulteta: Inštitut za kriminologijo pri Pravni fakulteti.

Khalid, M. A., Babar, M. I. K., Zafar, M. H., & Zuhairi, M. F. (2013). Gunshot detection and localization using sensor networks. In *2013 IEEE International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA)* (pp. 1–6). Kuala Lumpur: IEEE.

Komninos, N. (2008). *Intelligent cities and globalisation of innovation networks*. London: Routledge.

Lacinák, M., & Ristvej. J. (2017). Smart city, safety and security. *Procedia Engineering, 192*, 522–527. doi:10.1016/j.proeng.2017.06.090

Larson, C. (August 20, 2018). Who needs democracy when you have data? *MIT Technology Review.* Retrieved from https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/

Leydesdorff, L., & Deakin, M. (2011). The triple-helix model of smart cities: A neo-evolutionary perspective. *Journal of Urban Technology*, *18*(2), 53–63.

Maver, D. et al. (2004). *Kriminalistika: Uvod, taktika, tehnika* [Criminal investigation: Introduction, tactics, techniques]. Ljubljana: Uradni list Republike Slovenije.

Meijer, A., & Thaens, M. (2018). Quantified street: Smart governance of urban safety. *Information Polity*, *23*(1), 29–41.

Meško, G., Tominc, B., & Sotlar, A. (2013). Urban security management in the capitals of the former Yugoslav republics. *European Journal of Criminology*, *10*(3), 284–296.

Modic, M., Lobnikar, B., & Dvojmoč, M. (2014). Policijska dejavnost v Sloveniji: Analiza procesov transformacije, pluralizacije in privatizacije [Policing in Slovenia: An analysis of the processes of transformation, pluralization, and privatization]. *Varstvoslovje*, *16*(3), 217–241.

Mohammadi, M., & Al-Fuqaha, A. (2018). Enabling cognitive smart cities using big data and machine learning: Approaches and challenges. *IEEE Communications Magazine*, *56*(2), 94–101.

Mohanty, S. P., Choppali, U., & Kougianos, E. (2016). Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consumer Electronics Magazine*, *5*(3), 60–70.

Newburn, T. (2007). Understanding investigation. In T. Newburn, T. Williamson, & A. Wright (Eds.), *Handbook of criminal investigation* (pp. 1–10). Cullompton; Portland: Willan.

Orr, D. A., & Sanchez, L. (2018). Alexa, did you get that? Determining the evidentiary value of data stored by the Amazon® Echo. *Digital Investigation*, *24*, 72–78.

Palmiotto, M. J. (2013). *Criminal investigation*. Boca Raton: CRC Press.

Pereira, G. V., Macadar, M. A., Luciano, E. M., & Testa, M. G. (2017). Delivering public value through open government data initiatives in a Smart City context. *Information Systems Frontiers*, *19*(2), 213–229.

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. Santa Monica: RAND Corporation.

Peterson, M. (2005). *Intelligence-led policing: The new intelligence architecture.* Washington: US Department of Justice, Office of Justice Programs. Retrieved from https://www.ncjrs.gov/pdffiles1/bja/210681.pdf

Pillaipakkam, P. (2017). Data powers next-gen applications. In *Smart cities & utilities report: 2018 Black & Veach Strategic Directions* (pp. 33–36). Black & Veach. Retrieved from https://www.bv.com/sites/default/files/gated-content/strategic-directions-report/18-SDR-Smart-Cities-Utilities.pdf

Powell, A. (2014). 'Datafication', transparency, and good governance of the data city. In K. O'Hara, M.-H. C. Nguyen, & H. Peter (Eds.), *Digital enlightenment yearbook 2014: Social networks and social machines, surveillance and empowerment* (pp. 215–224). Amsterdam: IOS Press.

Public-private partnerships for SMART city management: Recommendations for local governments to prepare and implement SMART PPPs. (2015). Uraía Platform, UN-Habitat, & FMDV. Retrieved from www.uraia.org/documents/46/oct-2015-uraia-smart-ppp-eng_1.pdf

Ramaprasad, A., Sánchez-Ortiz, A., & Syn, T. (2017). A unified definition of a smart city. In M. Janssen, K. Axelsson, O. Glassey, B. Klievink, R. Krimmer, I. Lindgren … D. Trutnev (Eds.), *Electronic government* (pp. 13–24). Cham: Springer.

Ratcliffe, J. (2008). *Intelligence-led policing*. Cullompton: Willan.

Regulation (EU) 2016/679 of The European Parliament and of The Council. (2016). *Official Journal of the European Union*, (L 119/1).

Rich, S. (August 19, 2011). *Predictive policing project reduces crime in Santa Cruz, Calif.* Retrieved from http://www.govtech.com/public-safety/Predictive-Policing-Project-Reduces-Crime-Santa-Cruz-Calif.html

SeaSkate. (1998). *Evolution and development of police technology*. Washington: SeaSkate. Retrieved from http://www.ncjrs.gov/pdffiles1/Digitization/173179NCJRS.pdf

Sotlar, A. (2015). Reševanje varnostnih problemov – med nacionalno, lokalno in človekovo varnostjo [Resolving safety problems – between national security, local security and the safety of individuals]. In G. Meško (Ed.), *Varnost v lokalnih skupnostih zbornik prispevkov Prve nacionalne konference o varnosti v lokalnih skupnostih, Ljubljana, 27. november 2015* (pp. 26–33). Ljubljana: Fakulteta za varnostne vede.

Spencer, S. B. (2017). Predictive surveillance and the threat to fourth amendment jurisprudence. *Journal of Law and Policy for the Information Society, 14.1*, 109–149.

Stratistics Market Research Consulting. (2017). *Home security solutions – global market outlook (2016–2022)*. Retrieved from https://www.strategymrc.com/report/home-security-solutions-market-2016

Talari, S., Shafie-khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. (2017). A review of smart cities based on the internet of things concept. *Energies*, *10*(4), 421–444.

The British Standards Institution. (2014). *Smart cities – vocabulary*. Retrieved from http://shop.bsigroup.com/upload/PASs/Free-Download/PAS180.pdf

The Economist Intelligence Unit. (2017). *The safe cities index 2017*. Retrieved from https://dkf1ato8y5dsg.cloudfront.net/uploads/5/82/safe-cities-index-eng-web.pdf

The European Network of Living Labs (ENoLL). (n. d.). Retrieved from https://enoll.org

United Nations. (May 16, 2018). *2018 revision of world urbanization prospects.* Retrieved from https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480.

Willis, J. J. (2014). A recent history of the police. In M. D. Reisig, & R. J. Kane (Eds.), *The Oxford handbook of police and policing* (pp. 3–33). Oxford: Oxford University Press.

Završnik, A. (2018a). Algokracija: Od vladavine prava do vladavine algoritmov [Algocracy: From the rule of law to the rule of algorithms]. In A. Završnik, & L. Selinšek (Eds.), *Pravo in nadzor v dobi velikega podatkovja* (pp. 35–83). Ljubljana: Pravna fakulteta: Inštitut za kriminologijo pri Pravni fakulteti.

Završnik, A. (2018b). Big data: What is it and why does it matter for crime and social control? In A. Završnik (Ed.), *Big data, crime and social control* (pp. 3–28). London; New York: Routledge, Taylor & Francis Group.

About the Authors:

Kaja Prislan, PhD, Assistant Professor at the Faculty of Criminal Justice and Security, University of Maribor. E-mail: kaja.prislan@fvv.uni-mb.si

Boštjan Slak, Assistant at the Faculty of Criminal Justice and Security, University of Maribor. E-mail: bostjan.slak@fvv.uni-mb.si