Smart Security: Integrated Systems for Security Policies in Urban Environments

Enrico di Bella, Francesca Odone, Matteo Corsi, Alberto Sillitti and Ruth Breu

Abstract Smart Security systems are applications of the Smart City paradigm for local crime prevention. Like most Smart City tools, they consist of informational and technological components that support decision-making processes. A prerequisite for such tools is that they are supposed to be means of ongoing management and policy innovations: we therefore review some of the crucial components of a Smart Security system from the viewpoint of a local government or a local branch of the public administration, in order to analyze the high-level requisites, characteristics and potentials of such a system. The objective is to help Public officials in identifying both what defines a useful technical tool but also what is required on the part of the public administration to actually make it useful. We therefore discuss the following problems. First, we address the issue of indicators, data and the use of statistical analysis to infer the likely determinants of crime and to define risk parameters for urban spaces. In doing that, we suggest innovative tools to introduce spatial information in crime count models. Second,

E. di Bella (✉) · M. Corsi
Department of Economics and Business Studies, University of Genoa, Genoa, Italy
e-mail: enrico.dibella@economia.unige.it

M. Corsi
e-mail: matteo.corsi@edu.unige.it

F. Odone
Department of Informatics Bioengineering Robotics and Systems Engineering, University of Genoa, Genoa, Italy
e-mail: francesca.odone@unige.it

A. Sillitti
Center for Applied Software Engineering, Free University of Bozen, Bolzano, Italy
e-mail: alberto.sillitti@unibz.it

R. Breu
Institut für Informatik, University of Innsbruck, Innsbruck, Austria
e-mail: ruth.breu@uibk.ac.at

R. P. Dameri and C. Rosenthal-Sabroux (eds.), *Smart City*, Progress in IS,
DOI: 10.1007/978-3-319-06160-3_10,

we discuss sensors and sensor output analysis, trying to define the circumstances that make it useful and the new possibilities offered by current technology. Then we discuss about integration of different information both from a conceptual and a technical point of view, stressing the importance of closing the gap between cold and hot data in order to realize an integrated early warning system. Finally, we discuss the problem of creating a scalable Smart Security system in a local government, indicating a list of significant international experiences.

Keywords Crime mapping • Urban security policies • Security dashboard • Smart security • Intelligent video surveillance

1 Introduction

Smartness for urban environments is supposed to imply a commitment to innovation in technology, management and policy, but the first element of this triad has been researched within the "smart" framework more extensively than the other two [1]. This is the case as well with the specific dimension of urban smartness that is security [2]. Systems for crime visualization, analysis and street surveillance have already been proposed and researched theoretically and applied in practice (e.g., [3, 4]). From an IT standpoint, the gradual innovation regarding these tools has been mostly confined to the integration of different technologies and the development of new technical tools. In a few cases, authentically smart projects have aimed at innovating the management and the policies of urban security "together with" instead of "as a consequence of" the technology of urban security, but they have been few and far between [5–7]. Our intent is, therefore, to illustrate the structure, the logic, the objectives and the requirements of a "Smart Security" system from a management and policy point of view. The issues that we will cover are, of course, just as technical, but each single technical tool or methodology is going to be discussed from a problem-solving point of view, with greater focus on directing public administrations towards promising fields and less on suggesting hardware or software solutions for IT experts.

The foundational assumption of Smart Security is that to improve quality of life, city governance and management should be based on an exhaustive amount of information on a wide range of activities occurring in public spaces [8]. When collected consistently and in the correct format, such information may constitute the input of analytical tools allowing local governments to anticipate and understand economic and social processes and to respond effectively to issues, crises and environmental changes (e.g., [9, 10]). In the specific field of crime prevention, local governments are not always and not only the main actors of public security (depending on national systems) but also decision-makers for a number of social, economic and urban planning policies that can have huge effects on crime. Because of this, a Smart City approach dealing with urban security should be focused on translating theoretical knowledge about crime and deviancy into indicators, early

warning systems, models and analytical frameworks. Such a toolbox should then come into play when and where decision making takes place, supporting well informed, precisely targeted and correctly monitored policies.

In recent years, a number of large western cities have started massive investments aimed at innovating in the field of urban security and at building a better informational background to policy decisions about crime prevention, fear of crime and support to the more vulnerable components of the community (e.g., [7, 11]). There are, however, significant challenges to those efforts:

1. criminology offers a wide range of indicators concerning urban security, but most of them are disputed; different criminological theories suggest different ways of measuring crime, of measuring its determinants and defining the correct scale at which determinants should be identified;
2. behaviors and situations may be more accurate at defining crime then any indicator, but sensors meant to capture behaviors and situations either deliver information *post facto* or they are affected by a severe trade-off between accuracy and earliness;
3. indicators and sensors could theoretically work complementarily, both with the idea of extending the ability of a system to identify different and evolving threats and that of allowing triangulation [12]; however, integration of data sources of such different kinds is far from trivial and requires a consistent amount of planning and the cooperation of experts coming from different disciplines: criminologists, economists, statisticians, urban planners, video image analysts, and computer scientists;
4. even when information is available and reasonably accurate and timely, preventive action requires a lot on the part of the public administration; part of that is about technological innovation but a significant part is about management and policy innovation [1].

Smart Security should approach these challenges in two different ways: on one hand, it has to assume as relevant to its domain every technical solution that provides useful information and support to action for the Public Administration; on the other hand, it has to provide a constant evaluation of the consistency of each innovative tool with preexisting and preordained high level goals of innovative security policy and management. Conceptually, a Smart Security system consists of three logical units: the first one is the module for the analysis of "Place and Population", where crime is analyzed in conjunction with its macro determinants; the second one is the "Individuals and Behavior" module where it is analyzed at micro level and where the actions and movements of the individuals are relevant; the last module is the "Integrated System" software infrastructure which coordinates all the information flows inside the system and includes the user's frontend where most of the informative elements for the policy actions are shown. Compared to technologically-driven smart programs, Smart Security adds a virtual fourth element in the intense feedback between technological innovation and management and policy innovation. The new frontier in the field of Smart Security Systems consists of the integration of these partial elements in a single framework as the one described in Fig. 1.

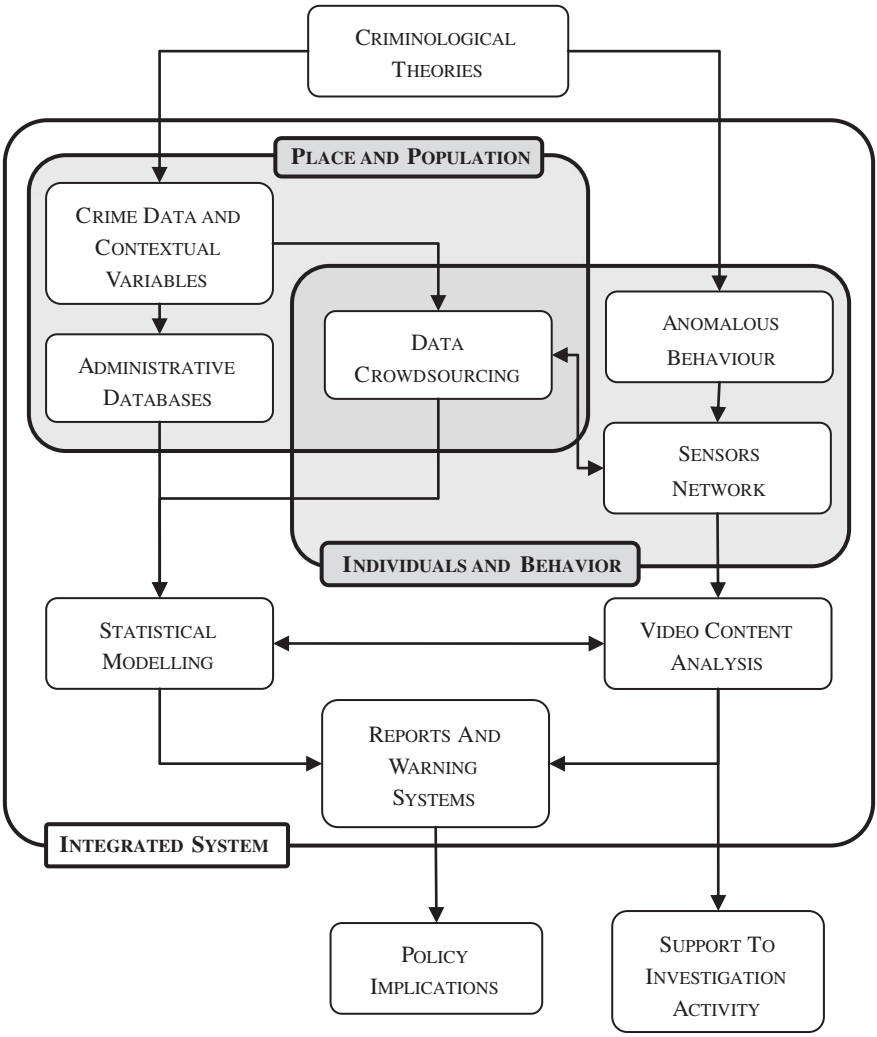

Fig. 1 Logical structure of a Smart Security Integrated System

2 Measuring Crime and Its Determinants in Urban Environments

Information concerning crime that is relevant to Smart Security includes measures of crime and measures of risk or mitigating factors. Such information may not be sufficient to create Smart Security systems, but it is all but necessary.

Like all measures, those concerning crime and its determinants are spatially and temporally located: they matter precisely because they provide intelligence about specific times and places. Since crime is not a constant over time and it is

not distributed uniformly in space, it is common practice to draw crime trends and crime maps [13]; these are two relatively trivial building blocks of any informative system (including Smart Security systems) designed to support decision making on urban security and both have a history that's at least a century old. However, as obvious as crime trends and maps are these days, they imply a concept that should be key to any innovative Smart Security system. The concept is that temporal and spatial clusters of crime are the "footprints" of local risk factors and local mitigating factors. It goes without saying that local determinants may change not only in size/intensity, but also in quality. So a Smart system is increasingly informative the more it is capable of mapping crime and its determinants at high resolution.

Measuring crimes is a less trivial activity than one might think: a crime is a legal (abstract) entity consisting of complex behaviors and multiple acts which are hardly numerable in most cases; a simple count of crimes requires therefore, a first level abstraction/elaboration that consists in identifying a reasonable proxy indicator for crimes (like calls for service, police incident reports, victimization self-reports, complaints, sentences, etc.). The raw number of crimes is rarely of use in support of management and policy decisions, as it is inadequate for cross-sectional and inter-temporal comparisons [14]; other indicators have been used in criminology and for official data and statistics, usually as an elaboration of a raw count of crimes, like population-based rates, risk-based rates, densities and location quotients. However, decision makers and public officials should be advised that different indicators actually indicate different things, that is, each proxy and each elaboration of the simple count of crimes carries with itself more or less sophisticated assumptions and meaning differences [15–23]. As for the indicators of risk factors and mitigating factors, a long and intricate debate has been discussing the determinants of crime since the early years of the discipline of criminology. The Department of Sociology of the University of Chicago is the source of the Social Disorganization Theory [24]. By studying the vast growth of the city of Chicago between 1860 and 1910, they noticed that urban areas were more crime-prone than rural ones. Moreover, they identified a connection between crime and several urban issues like poverty, racial heterogeneity, and residential mobility, all leading to the weakening of social control and the disintegration of formal social organizations [13].

The interest in geographic criminology began during the 19th century in France and in Belgium after the publication of the first geographical map of crime. In 1829, Michel Andrè Guerry and Adriano Balbi [25] published a map representing the distribution of crime over the Departments of France between 1825 and 1827. This preliminary study was followed by that of the Belgian statistician and astronomer Quetelet in 1842 and by a number of studies in the Netherlands, England and Wales and in Italy [13].

Between the 60s and the 70s several authors (e.g., [26–28]) developed analytical frameworks of crime and insecurity in the urban environments focused on spatial and functional features of the built environment. Their work, which is globally labeled as the Ecological Theory of Crime, is the combination of very different approaches (Crime Prevention Through Environmental Design—CPTED, defensible space, eyes on the street, etc.).

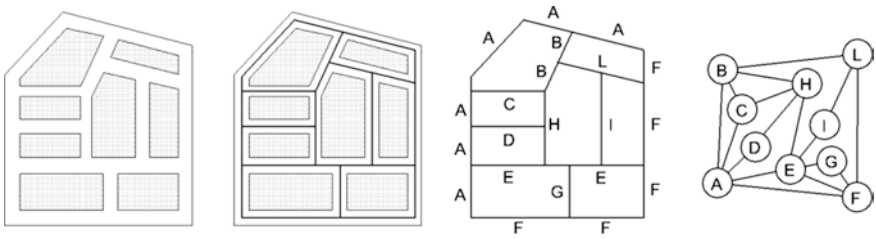

Fig. 2 Dual representation of the urban map. From the *left* to the *right* a simple urban space made of buildings (*shaded shapes*) and roads; the median lines network of the streets among the buildings; the roads network (letters stand for the street names); the graph corresponding to the original urban layout based on the street crossings

These ideas paved the way, during the 80s, to the development of situational crime prevention [29–32]. According to the followers of the situational crime prevention, to reduce the number of crimes, it is necessary to reduce the opportunities of committing a crime because "opportunity makes the thief" [33]. These ideas led crime analysts to increase the attention for urban design details (such as street furniture, street lighting, pedestrian pathways, housing design, visibility from the street and of the street) and to a deep study of the spatial configuration of the streets conducted through the Space Syntax Analysis (SSA) [34]. SSA was initially conceived as a theory to analyze small environments and their configurational features. This discipline studies the configurational properties of urban space [35] through quantitative measures. Thus, it allows the identification of patterns and structures which influence the development of activities in space, in particular movement and land use [36]. Figure 2 exemplifies for a simplified urban structure how it is possible to convert an urban layout (first figure on the left) into a graph (last figure on the right), a mathematical object whose characteristics can be measured in many different ways (e.g., [37]). Since movement and land use are thought to be linked to crime, SSA was used in the development of the CPTED proposed by Jeffery [28]. Thanks to the increasing number of measures used in the Space Syntax Analysis, it soon became possible to compute the relative degree of accessibility, connection, and integration of each street in its urban network, and to index numerically a large number of properties of the urban environment [36]. Among the others, [38] analyzed the street structure and its dependence with crime volumes: they found that streets with many twist and turns have higher crime rates.

During the last thirty years, a new theory on the spread of crime through urban spaces emerged. According to the Routine Activity Theory (e.g., [39]), the number of crimes increases if the number of opportunities for criminals rise and if society lacks an adequate surveillance against crime. Indeed, crimes are often committed in places where victims and offenders hold their routine activities, for example work, leisure, or social interaction, and where they satisfy their basic needs [40]. This theory focuses on space because it is considered an explicit determinant of human actions, including committing offences. Some

empirical studies are in favor of this theory [39]. Used Routine Activity Theory to explain the increase in the number of crimes in American cities. For instance, they pointed out that, with more women working, a larger number of houses were empty during daytime and this fact led to the rise in the number of robberies increasing the vulnerability of suburbs [41]. Found out that, in Cleveland, streets with schools and bars are highly crime dense, while [42] identified the places near commercial stores as particularly risky. In this context, some studies on the relationship between crime and transports have been developed by [43]: they conclude that the structure of the public transport system can influence the number of crimes committed: higher numbers of crimes are recorded near stations and bus stops.

In recent years, a new interest for a combined study of socio-demographic and spatial factors in the analysis of crime has emerged. In fact, although crime mapping is certainly the most immediate way to obtain quick information on the criminal incidence in an area, it is interesting to study the relationship between urban crimes and the economic, socio-demographic and spatial features of the study region. Indeed, the study of crime in the context in which it happens could bring to the identification of both global and local risk factors, helping local governments in drawing up policies for Urban Security [44]. Provides empirical evidence for skepticism on the idea of "territoriality" and "defensible space" put forward by Newman [27]: he suggests that, other things being equal, property crimes tend to cluster in those globally or locally segregated areas. In detail, particularly risky areas can be found in cul-de-sac footpaths and rear dead end alleys, but also in those segregated short cul-de-sac carriageways which Newman considered to be the key places where local surveillance should be increased and casual intrusion by non-residents excluded. Hillier [45], discussing the work by Chih-Feng Shu [44], concludes that in Space Syntax Crime Analysis, spatial factors are relevant and that they operate both at a global and local level. More recently, [46] discuss the relationship between crime and urban planning presenting also the results of an empirical research conducted in the city of Vilnius: the aim of this study is to identify, with the use of ASA, the most vulnerable open public spaces of the city.

3 The Role of Statistical Analysis in Integrated Systems for Smart Security

Information of the kind presented in the previous paragraph becomes relevant to Smart Security systems when it allows local governments and the public administration to monitor the development of the situation, to infer plausible causal relationships between some theoretical determinant of crime and a certain measure of crime and when it allows either to identify promising actions that can be taken or situations that cannot be explained under the available information and require additional investigation. From a statistical standpoint, it means being able to

produce basic descriptive statistics of crime and being able to produce statistical models. The basic statistics of crime are little more than the conceptualization of crime trends and crime maps: means, rates, standard deviations, spatial and temporal clusters, etc. These are the most commonly and widely used tools for the statistical analysis of crime and they let public administrator monitor the evolution of crime over time or compare crime rates in different areas, they do not include any interpretation of the counted events, neither suggest possible policies or actions that may be appropriate or useful. The availability of microdata that contain georeferenced information on relevant risk factors at street level of detail, allows a second, more effective level of analysis. The database of reported crimes, made of records containing a full set of the available information relating each crime (e.g., date and time of the event; gender, age, and nationality of the victim; place of the event; etc.), can be combined with all the other information that Municipalities possess for their administrative purposes.[1] Therefore, criminal events recorded by law enforcement agencies and risk factors suggested by criminological theory can be analyzed conjointly (e.g., [47]). Statistical models identify which contextual variables actually work as risk factors or mitigating factors and can be considered as explanatory variables with crime being the dependant variable. The interpretation of the model starts with the estimation of a set of coefficients, one per explanatory variable, which mediate their effect on the criminal occurrences over the whole city; the coefficients may be positive or negative depending on their role of increasing or decreasing crime risk. Thanks to the model, it is possible to compute for each spatial unit (street, street segment, block, etc.) a number of expected events based on the values of the contextual variables and to compare these expected events to the actual number of recorded crimes. In principle, even with important objections that, for the sake of simplicity, it is unnecessary to delve here, this difference among these quantities is a measure of goodness of fit of the model. As a general rule, if the criminological hypotheses fit well to the specific study area, most of the roads should have an expected number of criminal events that is close to the actual number of occurrences. On the contrary, high discrepancies among these values may identify situations with far fewer events, or too many events than the ones expected on the pure basis of the context variables values. The first situation suggests the presence of unspecified favorable conditions unaccounted for by the model: some relevant

[1] Possible examples are demographic elements (e.g., number of residents per age interval, gender, and nationality), socio-economic indicators (e.g., house values acquired from the Land Registry, aggregate tax return values, number of shops, number of gambling halls, number of bars and pubs, etc.), or configurational dimensions of urban spaces as they result, for instance, from the Space Syntax analysis (centrality of the street in the urban network, pedestrian movement, number of intersections of the street with other streets, etc.) or from the CCTV measurements.

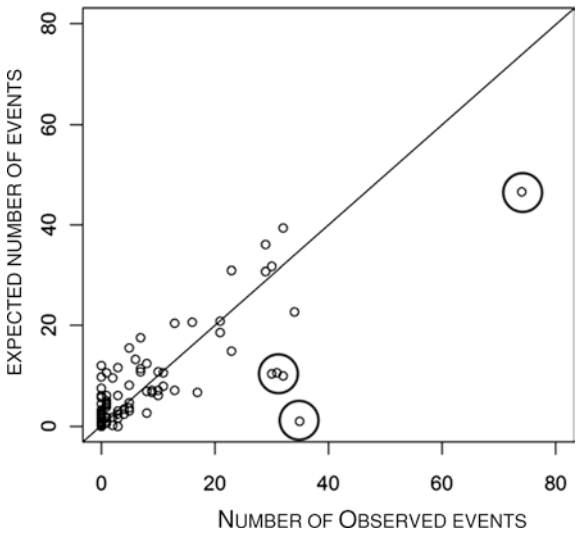

Fig. 3 Expected versus Observed arson and criminal damage occurrences on parked vehicles in a neighborhood of an Italian city in a 24 months period. Circled are the "soccer stadium effect" roads

factors that are omitted from it seem to actually mitigate crime. The area, in this case, is worth a specific investigation as its crime-mitigating characteristics might be be reproducible elsewhere in the city and used as positive experiences, as long as a later on-the-field analysis is able to identify the positive factors at play. In the second situation, we have a number of events that is much higher than expected and there are some elements, unspecified in the model, increasing the actual risk of the road. Figure 3 shows an example of a comparison between observed and expected values for the number of damage recorded for each street in a neighborhood of a city in northern Italy. The more the points (representing the single streets of the neighborhood) are positioned along the diagonal, the better the matching of the expected versus observed values. On the contrary, the more they move away from the diagonal, the stronger the effect of the contextual elements not included in the statistical model. In a Smart Security System, a statistical module with the characteristics herein described and whose skeleton structure is given in Fig. 4 allows local administrations to identify critical situations for which customized solutions are needed.

In addition to this, the literature of statistical methods for the analysis of crime is very vast and may be helpful to investigate the effect on crime of intervention policies, of new technologies, of social change or urban planning. For a recent review of these techniques, refer to [48]. The statistical tools can be properly customized to answer the needs of any municipality. However, it is relevant that when a Smart Security system is implemented, the key points that the Public Administrators need to check and monitor are clear and well defined in the system design phase: statistical analysis does not make sense by itself; it should be shaped around the information needs of law enforcement agencies.

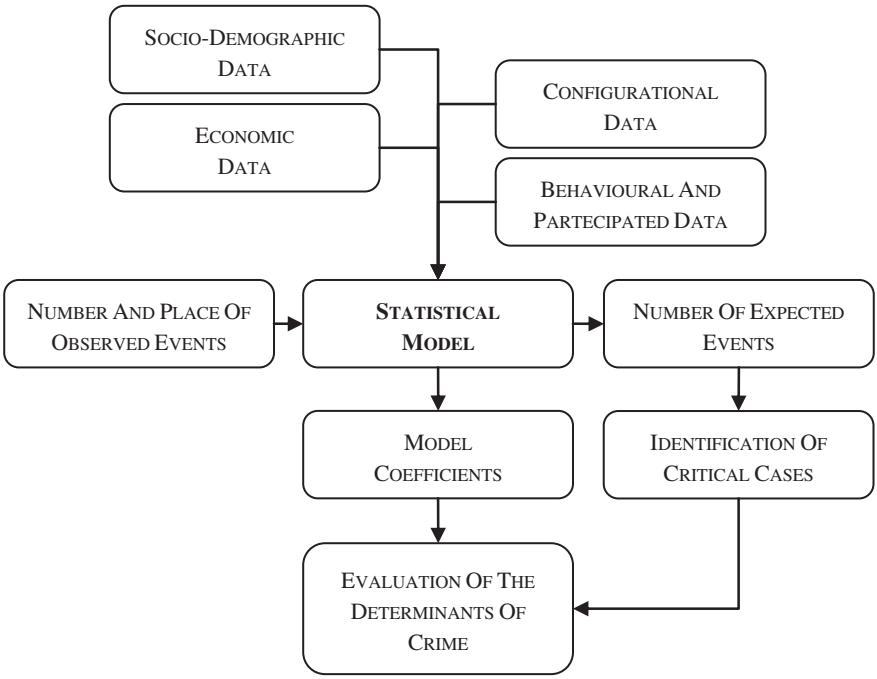

Fig. 4 The role of statistical modeling in the analysis of crime

4 Individual Behavior and Sensors

Sensors are supposed to have a crucial role in Smart City [49, 50] and the domain of Smart Security benefits from theories and practices concerning the use of sensors for crime control that predate the concept itself of Smart City by a few decades. Optical sensors are the most obvious example: the first experiments of video surveillance systems for crime prevention date back to the 80s. However, motion detectors, acoustic detectors (like gunfire locators) and even biological and chemical sensors all have been considered for their potential in crime prevention and repression strategies. The rationale behind the use of sensors in a crime prevention environment has usually been that of detecting individual behaviors, with the purpose of collecting evidence (in a forensic perspective), directing prevention or repression efforts against crime acts or deterring crime altogether by virtue of the mere possibility of collection of evidence and activation of preventive and repressive actions. In a Smart Security environment, the value of evidence collected through sensors is assumed as a given in the same way crime maps and trends are. Smart Security begins where the benefits of preventing crime, instead of repressing it, come into play. The evolution of video surveillance is paradigmatic with respect to the problem of deterrence, repression and prevention. For many years CCTV systems have been very controversial and their effectiveness for crime prevention has been questioned. While law enforcement agencies worldwide have been

investing for years in CCTV as a crime-fighting technology and the technology behind CCTV rapidly developed and cameras proliferated, supporters of CCTV have typically argued that cameras make cities safer but recent studies have called into question this claim. According to some, their effectiveness might be limited and their impact on citizens' sense of security might be the opposite of what governments intend [51–56]. Surveillance systems have been welcomed by public administrations for monitoring purposes (parking lots, public transports), for access control (automatic car plate reading, etc.) or transport security [55]. In July 2005, during the attack to the London subway system the public video surveillance system installed allowed the authorities to identify the bombers and trace their paths. The system did not prevent the attacks but its help in subsequent investigations was priceless. This event encouraged public administrations to invest on video surveillance systems to prevent crimes and terrorist attacks. Since then, the scale of video surveillance networks has increased in scale [57] and today installations of 50,000 camera networks have been reported. The Singapore transport network is monitored by a 6,000 cameras network and, in general, most urban centres can count on camera networks of dozens of cameras.

These large systems are usually connected to centralized control centres, where a human operator interacts with dozens (or hundreds) of sensor sources using several separate monitors/windows for visualizing and analyzing the video or data streams. Although each separate source produces useful data, the human operator is easily overwhelmed with the task of integrating these varied forms of data into a complete global view and understanding of a scene.

This scenario will soon become obsolete thanks to the technological progress of intelligent systems and algorithms [57]. Indeed, the proliferation of surveillance cameras throughout public places stimulates the development of software able to monitor automatically the large amount of video footage produced. Human operators cannot monitor such a vast volume of data. This means that today most large installations have a limited effectiveness because of the lack of means to interrogate the content of the data generated. Once a camera network is installed, it is important to estimate the topology of the network to learn the relative positions of the cameras and the possible intersections between fields of view. This simplifies various tasks, among all an effective tracking of people within the space monitored by the network. The topology cannot be estimated manually if the network is large. Automatic procedures may also be applied to facilitate the design of the network: locate optimal positions of the camera for a maximum coverage [58].

Such networks are often heterogeneous as they often include cameras installed by the public administration specifically for the purpose of public security, plus private camera networks that may usefully complement the available information, such as cameras installed by ATMs, banks, stores, etc. This heterogeneity on the sensors, the transmission, and compression protocols, causes additional problems, producing asynchronous videos (e.g., [59]) and variable resolution signals.

Modern camera systems are able to control large areas, to zoom in (with optical zooms as in PTZ cameras or digitally, with mega or giga-pixel cameras), but also to detect moving objects and track them along the scene [60]. These systems perform real time analysis and, more importantly, record video footage for later use.

Information acquired by multiple cameras may be merged with the purpose of tracking moving objects across the views [61, 62]. If cameras have a field of view overlap one may associate corresponding view simultaneously. If the cameras have no field of view overlap moving objects may be associated along time based on an analysis of their similarity and on prior knowledge on the cameras mutual positions [63, 64].

In crime prevention, video surveillance is closely connected to biometry, since the ultimate goal is often to associate a face to the person who perpetrated the felony. Face biometry (i.e., the ability to associate automatically an identity to a face portrayed in an image or image frame) is particularly attractive, since it does not need any specific sensor but can be applied to the output of a high resolution video stream. The research community has been very active on this respect, addressing face recognition from different perspectives (e.g., [65]). Although the achievements on face biometry in the last decades are impressive, satisfactory results can be obtained mainly in constrained scenarios or with a relatively small set of enrolled identities and, for this reason, the use of face recognition in urban environments is still limited [66, 67].

Early intelligent video surveillance systems were able to detect the presence of people in forbidden zones. This was the extent of the forbidden/dangerous action taken into consideration. Nowadays, we are concentrating instead on dangerous behaviors of people and crowds [68–70]. More recently, the interest of the research community has been directed towards intelligent systems able to learn models of normal activities from long time observations and to apply them to detect anomalies in an adaptive way [71–74].

5 Where All That Is Observational Converges: Smart Security as a Preventive and Early Warning System

A Smart Security system should be designed to work at the point of convergence of multiple information sources. From what has been discussed so far, it is clear that some sources are “cold” data collected by various structures of the Public Administration; others are hot and consist of live raw or processed information coming from sensors situated in specific locations in the urban area.

An additional and very important source is a hybrid of the two: crowdsourcing[2] allows local governments to receive massive amounts of data, reports and contents generated via smartphones and the internet in general [76, 77]. Crowdsourcing can

[2] From a terminology standpoint, this entire field is still lacking consistency. We make use of the term “crowdsourcing” in its more general meaning of an organization outsourcing specific tasks (like producing goods, services or information) to vast crowds of unrelated individuals instead of using traditional employees or suppliers. As a matter of fact, the term is frequently associated with the generation of web contents because that was the first practical application of crowdsourcing [75], but a broader meaning should be acceptable as well. Specific forms of crowdsourcing that are particularly significant for Smart Security systems have specific names, like Crowdsensing or Smartsensing, that imply the use of ubiquitous sensors (mostly smartphones) to collect data.

integrate, in a vast number of fields, the traditional information used by the Public Administration [78–81] and it surely can mitigate the cost of building large networks of sensors while producing information that, being collected on the end user-side of the public services supply system, can be much more contextual (i.e., rich with information about what is being sensed, where and when, beyond what a single sensor is normally expected to capture).

A much debated issue concerning data from smart sensing tools is that of privacy. While this is a very serious and relevant problem, it is not substantially different from that of privacy with all the rest of geo-localized or remotely-sensed information that local governments already use (e.g., in G.I.S. systems). So, while the specificities of smart sensing have to be considered also under a privacy perspective and while privacy is obviously an issue when a smart system uses data concerning individual citizens, the hypothesis of using such systems seems to mostly require specifications and not innovations of existing privacy rules. Privacy and anonymity issues influenced the spread of public video surveillance systems [82, 83]. In most countries, current legislations do not prevent abuse or misuse of video footage. Misuse can be perpetrated by individuals with an access to the video stream or by organizations. While the debate is still open, to some extent, technology is offering different ways of protecting the privacy of citizens: face detection or text detection can be used to anonymize video footage [84], video encryption technologies allow us to protect video sources [85]. If these filters are implemented within the sensors, thanks to the use of embedded systems, then the video stream is protected from the source and can be transmitted safely.

Crowdsourcing is a significant addition not only because of the scope of its reach but also because it shows that a rigid distinction between hot and cold information limits the smartness of a system. Live sensors should be used to generate cold data as well [86]. Statistical analyses over time periods should help decoding the meaning of what a live sensor is capturing. In broader terms, in a Smart Security system there is relative continuity and exchange of information between the analytical environments of what has happened in weeks, months or even years and what is happening now or is going to happen in a few minutes. From the point of view of a Local Government or that of any local branch of the Public Administration, Smart Security is, in fact, an early warning system (or the premise of it) precisely by virtue of this integration of information relative to different timeframes. Early warning systems (EWS) are "The set of capacities needed to generate and disseminate timely and meaningful warning information to enable individuals, communities and organizations threatened by a hazard to prepare and to act appropriately and in sufficient time to reduce the possibility of harm or loss".[3] EWSs have been implemented in many fields, from disaster management and prevention to epidemiology, drug control, poverty reduction, drought and famine prevention, armed conflict prevention and so on. In the field of crime prevention, EWSs have been used to organize

[3] United Nations, Office for Disaster Reduction (UNISDR).

policing [87–90] and to predict individual behaviors [91]; while the concept is popular, however, its application in complex governance problems is only becoming feasible in current Smart City environments.[4]

In a Smart Security system, statistical tools, sensors and crowdsourcing information, integrated with each other, produce an output that consists of the synthetic results of the analysis performed by each, and of a system of flags that appear in front of the system managers when certain trigger conditions are met. For example, it may happen that the recent history of a place shows a particularly intense spatiotemporal concentration of crimes, or that the trend of its socio-economic and demographic characteristics that are likely determinants of crime may hint at a probable increase of the risk of crime. The objective of the smart tool is to communicate what the flag is about in simple, unambiguous, and exhaustive fashion, adopting output representations that can be easily interpreted by city officials that are responsible of the decision making process. More precisely, flags should be designed to be the first element of the decision making process at the end of which the Public Administration produces a policy change or an action of some sort to improve urban security conditions. Given these requirements, a smart tool for urban security adds to the units of analysis an interface for the management and the representation of data that is built around three distinct elements: a crime map, a dashboard, and a warning system. The crime map is the most basic level of the entire system; it is meant to allow the spatial representation of crime but can as easily be used to map relevant context variables, in particular when they show some correlation with the presence of crime or to illustrate composite indicators. Since one of the objectives of the unit performing the statistical analyses is modeling urban crime and then showing the difference between estimated and observed values, such estimated values and difference of values are two particularly significant examples of composite indicators. The crime map can have any sort of definition level, from that of large administrative subdivisions to that of a single street or street segment. Since the main objective of the map is to make apparent any geographic effect at play, it has to show how the concentration of each relevant variable changes from place to place, making the dislocation of high and low values more important than the values themselves. This usually means that the value of a variable in each geographical unit is synthesized through one out of a finite palette of colors (four to ten in most cases) and the overall chromatic patchwork created by the map should give, in a glance, the idea of dispersion and concentration. Dashboards represent the second level of the interface. They provide a different method to read the values synthesized on the map with less emphasis on the spatial effects and greater emphasis on ranking and prioritization, discrimination, and detailed comparison. Dashboards are intended to quantify the measure of significant variables, usually within a graphical representation that

[4] See [92] for a current commercial example. Similar examples can be found concerning predictive policing and disaster management.

helps interpreting the value, for example by adding a scale of colors ranging from green to red depending on the measured value. While apparently simple, dashboards imply some intricacies: the top and the bottom of the scale may be fixed or depend on historical longitudinal observations or on current cross-sectional values, with the average and the thresholds between low and average and average and high that change accordingly. Obviously, the difference is not only the different outcome but also the different meaning: measuring a value against its historical highs and lows is different than measuring it against the values of the same variable in different places. A dashboard can also help visualizing the difference between the current value and the value recorded in the previous time unit, from a few hours or days to months before, giving an immediate representation of change. The numerical values of a variable, of its change over time or its difference with the values in other places, allows decision makers to set priorities for their actions on one issue or to balance the effort between different issues. Dashboards allow to easily identify and list places where the value of a variable is above or beyond a certain level and to disentangle the effects of different explanatory variables on a dependent variable. This makes possible to understand which risk factor is high where actual crime is high or which risk factor is responsible for making expected crime high. Dashboards should be contextualized as much as possible: since they are an extremely synthetic tool, the user should be given as much information as possible on the characteristics of the place that the dashboard refers to, so that the reading is not left as an abstract and inexplicable value. Usually, maps and dashboards contain quantitative information on places and population. However, smart sensors and cameras, while primarily oriented to analyze individual behavior, are also a source of cumulated individual behaviors. Therefore, if a smart tool for urban security is built around them, a considerable number of variables that can be represented in maps and dashboards can actually come from a database of what was captured by smart sensors. The last element of a smart tool is a warning system. It can exist as a specific element of the tool or it can be integrated within the map and the dashboard. Its function is to help the user at noticing critical situations even when they are hidden in a large amount of information, indicating it with a flag, i.e., a specific and visible signal of some sorts. Flags may be the consequence of slow, gradual processes that progressively increase risk at a certain place beyond a given level. They may come from sudden increases, from cyclical peaks and they may as well depend on individual behaviors that are excessively distant from the average or from an accumulation of many concurrent and slightly anomalous behaviors of different people. Flags are not particularly sophisticated instruments; they are based on threshold values that trigger them when the reading goes above or below. The sophisticated part of a warning system is the balancing of the thresholds, of the sensitivity of the triggers, and the ability of the system to react to changes by updating its thresholds over time. Obviously, the objective is minimizing false positives as well as false negatives, keeping in mind that a smart tool is not a substitute of decision makers but just a support system and, consequently, whenever it is possible, flags and warnings should stimulate a cross-checking of results and an on-the-spot investigation before any actions are taken.

6 Handling Complex Systems: The Integrated Network System

Integrating information from different sources is a very complex activity, especially if the data sources are very different from each other (e.g., text, video, audio, etc.). To simplify the integration processes, sources other than text often need to be enhanced through the manual or automatic generation of meta-data that is a textual description of the content of the data source (e.g., the name of the people in a video, the date of the data collection, a transcript of the conversations from the audio, etc.) [93]. However, even in the simplest case in which we need to integrate only text-based information, the activity can present several challenges.

Moreover, there are several kind of information coming from different sources that can be integrated and used to improve the situation awareness (e.g., weather, air quality, light, etc.) that can provide a constant (and frequently large) stream of data. The amount and the heterogeneity of such data is extremely difficult to manage with the traditional approaches based on OLAP (On-Line Analytical Processing) and data warehouses [94]. To this end, new approaches have emerged and classified under the label *big data* and implemented through the so-called NoSQL databases [95].

On-line analysis of data is also required to ensure the reliability of sensors used for the data collection to identify immediately problems that may prevent useful subsequent analysis and integrations with other sources. Such analyses include simple statistical evaluations of the quality of the data and complex ad-hoc analyses based on the information coming from different sources that are related to each other and can be used to crosscheck their validity. The quality of the data collected is the starting point for implementing an effective integration reducing false positives and false negatives, therefore an alerting system based on on-line analysis can help in such activity.

To have complete information integration on which it is possible to develop reliable applications, it is required that the integration is implemented at different levels: communication, syntactic, and semantic [96]. The communication level deals with the technical aspects of the data transfer among the different systems involved in the integration; the syntactic level deals with the data formats and the transformations required to create a common representation of the information; finally, the semantic levels deals with the meaning of the different pieces of data and how to relate each other.

At each level, there are several challenges including the followings:

Communication level	size of the information and technical implementation
Syntactic level	kind of information and storage
Semantic level	organization of the information

The organization of the information deals with the ability to define high-level (and generally abstract) concepts and connect all pieces of information related to that concept. For instance, considering a robbery, there are several pieces of

```
<AGENDA>
  <PERSON>
    <NAME>JOHN</NAME>
    <SURNAME>SMITH</SURNAME>
    <EMAIL>SMITH@ENT.COM</EMAIL>
  </PERSON>
  <PERSON>
    <NAME>TOM</NAME>
    <SURNAME>BROWN</SURNAME>
    <EMAIL>TB@BROWN.COM</EMAIL>
  </PERSON>
</AGENDA>
```

```
<LIST>
  <CONTACT>
    <NAME>JOHN SMITH </NAME>
    <EMAIL>SMITH@ENT.COM</EMAIL>
  </CONTACT>
  <CONTACT>
    <NAME>TOM BROWN </NAME>
    <EMAIL>TB@BROWN.COM</EMAIL>
  </CONTACT>
</LIST>
```

Fig. 5 Incompatible structured information providing the same content through different structures

information from different sources that can be related including: the timeframe from the police reports, the suspected invited people from the investigation records of the police, the video of the surveillance cameras, etc. Such integration is very difficult to perform automatically and requires an extensive amount of research to be implemented in a general context even if in some very restricted domains it is feasible with the current technologies that are part of the so-called *semantic web* (even if the term includes the world "web", the technology is not used only for the web but it is the domain where it comes from) [97].

The kind of information refers to its structure. We can classify information in two large sets: unstructured and structured. Unstructured information is any kind of text designed with human beings in mind (e.g., this book). On the contrary, structured information designed to be processed and stored easily by a machine through a database and exchanged using a semi-structured form that includes special markers (called *tags* in many languages used for this purpose) that makes processing possible. Languages like HTML (HyperText Markup Language) and XML (eXtensible Markup Language) are very popular in any kind of document-based representations (not just on the web for which they were conceived at first) and are based on such a concept to make the interpretation, the visualization, and the storage of information easier. However, even with structured and semi-structured information, the integration of different data sources is not straightforward since each source may use a different set of tags and organize the information in different ways. In Fig. 5 an example of two incompatible structures of the same information is given. Moreover, it happens very frequently that the differences among data sources are not just syntactic differences (Fig. 5) but also semantic ones (e.g., the same tags used to identify different content in different documents, different in information sets provided, etc.). Therefore, integrating different data sources requires a deep knowledge of the data representations and requires a considerable effort. However, given the importance of the applications that are based on information integration, there is an enormous amount of research in the area aiming at automating the

integration as much as possible [98, 99]. One of the current trends in research about information integration is based on the development of ontologies that allow automatic conversion mechanisms and highlight incompatibilities [100].

How the information is stored and its size are additional aspects that need to be considered when dealing with different sources of information. Currently, every activity (human-based or machine-based) produces a large set of digital information stored in several databases. Such databases are huge, therefore transferring or copying the entire data sets to perform complex operations is often unfeasible. Beyond such problems, we also have to consider the sensitivity of some kind of data and/or the privacy aspects related to them. In such cases, a sanitization procedure is often required before allowing other kind of operations and analysis on such data removing the sensitive part of the data and/or aggregating at a higher level with no privacy or sensitivity concerns.

Therefore, it is required to develop on-line analysis techniques that are able to process and integrate information on the fly (whenever such information becomes available) and exchange only the relevant data without overloading the communication infrastructure. Moreover, relational databases that are often used to store information struggle in managing such large amount of data if there is not an adequate investment in the hardware infrastructure. As stated before, traditional approaches through data warehouses are not able to address properly this kind of problems, therefore NoSQL databases are emerging offering better performances and scalability at a much lower cost at expenses of some properties of the relational databases that can be relaxed in some application contexts. These technologies have been designed to address problems related to the storage of large data sets but their correct usage is linked to the specific problems the application has to address.The technical implementation is basically related to the usage of specific technologies. In the well-known world of relational databases, there are standards that are accepted by almost any implementation such as the SQL language to perform interrogations and insert/modify data. However, in the NoSQL world, there are no common standards for even basic operations and each implementation has its own approach producing two main effects: 1) it is difficult to switch from one technology to another and 2) every technology requires a complete set of new skills. For this reasons, the use of NoSQL technologies need to be considered only in specific cases since it may be difficult to fix some mistakes in the selection of the right technology to use.

There are plenty of open source technologies that can be used to implement such systems (databases, analysis and visualization tools, sensors, etc.) producing a set of advantages such as the absence of a license fee, the ability to adapt the tools to the specific needs, no vendor lock-in, etc. Moreover, when dealing with problems related to integration, security, and privacy, the usage of open data formats, protocols, and tools help in identifying bugs, assuring the absence of malicious code and enhance the overall interoperability and the level of integration of different systems.

From the architectural point of view, integrating several data sources at the same time is extremely complex due to the main problems described earlier. However,

the technologies available today allow developers to split the problems in several smaller problems that are easier to address and integrate them only later on. In this way, it is possible to create a more scalable architecture able to integrate an arbitrary number of data sources limiting the complexity of their integration. In any case, even with just two data sources, the three level of integration (communication, syntactic, and semantic) should be taken into consideration to provide a meaningful integrated system.

A specific issue related to the integration of video sources requires a reference to interfaces, in particular when IP video cameras are concerned. Over the years the main producers developed various standards, currently the main one is ONVIF, founded by Axis, Bosch and Sony. ONVIF is about (1) standardization of communication between IP-based physical security devices and (2) interoperability between IP-based physical security products regardless of manufacturer. It is also worth mentioning HD-Serial Digital Interfaces (SDI), a family of digital video interfaces used for transmitting uncompressed, unencrypted digital video signals within analog television facilities. This technology has been conceived with the goal of bridging the gap between analog systems and digital installations over IP.

7 A Good Start: Roadmaps Towards a Smart Security

With all the different issues now on the table, we can conclude our work with an attempt at drawing guidelines for the implementation of a Smart Security system in a Public Administration context. Smart Security tools may have different levels of complexity, having to comply with different technical, administrative, and economic limitations (see Table 1 for a few documented examples), but some elements in their infrastructure and implementation are going to define if and how much they can actually be considered smart.

The first and crucial element that defines the smartness of a crime prevention system is that it should be built around the management and policy needs of the Public Administration and not as a retrofitting of them. "Technological performance is not to be taken for granted as a logical progression from technological advancement, but rather performance depends on effective management of technological systems and infrastructure" [1]. The bottom-up process of influential projects like COMPSTAT [101, 102], GeoArchive [87] and the general effort to introduce GIS as a crime prevention tool [4, 103] constitute very good examples.

Being an early warning approach, Smart Security requires an "early response" organizational framework as well. This means that, regardless of the source of the information that generates the warning (be it a statistical analysis, a live sensor, a crowdsensing tool or a triangulation combining any of them) the organizational goal must be that of having the resources required to prevent the issue and the determination and ability deploy them in a timely fashion.

Table 1 Existing projects and software containing significant smart elements

Notable examples	Smart elements
Compstat [101, 102, 104, 105]	Organizational focus, bottom-up development, data collection, mapping, statistical analysis, early warning philosophy, results evaluation
GeoArchive [4, 87]	Organizational focus, bottom-up development, data collection, mapping, statistical analysis, early warning philosophy
SACSI [106–108]	Data collection, mapping, statistical analysis, results evaluation
COMPASS [109]	Data collection and data sharing, mapping, statistical analysis, decision support, results evaluation
Operation virtual shield [100, 110]	CCTV, early warning philosophy
G.I.S.-based free and commercial software [103]	Mapping crime and context (with elements of statistical analysis)
Urban crime simulator [111]	Crime modeling based on criminological theory
Desurbs [7]	Organizational focus, data collection, urban planning and design focus, mapping, statistical analysis, decision support, integration
Commercial software (PredPol, IBM Spss and BlueCrush, Esri, …)	Mapping, statistical analysis, predictive policing

In terms of components, a Smart Security system is scalable according to evolving needs and consists of part or all of the following key elements:

1. Relevant administrative databases (e.g., crime records, socio demographic and economic data, urban graph);
2. Sensor network(s);
3. Crowdsourcing applications and websites;
4. Crime maps and trends visualization;
5. Security dashboard;
6. Intelligence module (Data integration and analysis).

The entire system, in order for the early warning mechanism to work, has to be integrated inside a single user interface with coordinated warning flags. However, of all these elements, some may already be in use in many local governments and just need to be integrated in the new system, while others require a greater deal of work. In spite of this, incremental developments are possible and, in many ways, superior to the "all-or-nothing" approach. Another crucial point is that Smart Systems are, by definition, tailored locally and, consequently, they do not necessarily need every element of this list. Some smaller settlements may never have enough data to justify a complex statistical tool. Some may have little need for having both a crime map and the dashboard. Sensor networks are a useful addition where and when their effectiveness is documented and sensors are worthwhile if there is a precise idea of what use to make of the data collected through them.

With respect to point 1, the main problem which may arise is technical, due to the existence of databases which are not normalized and which make difficult their

querying or joining. Classical examples are different geographical boundaries of the statistical units, different levels of aggregation of data, different definitions of the same variable, coding errors caused by fields that are sensitive to spelling mistakes or different forms of abbreviation. Concerning point 2, most of the Municipalities interested into the implementation of a Smart Security system already have a CCTV system of cameras installed and it is usually reasonable to integrate an existing infrastructure into the framework of a smart system whenever possible. However, there is no guarantee that the technological standards and the aims of such an infrastructure are ultimately compatible with a smart system. Crowdsourcing and smartsensing projects (point 3) are currently being developed in some of the most advanced and innovative municipalities around the world, but compared to other elements of the system, here the emphasis should be on designing them with compatibility with a Smart Security environment in mind from the beginning. Whether they ask users to produce content, ideas, information or else, in a proactive creative process or they just ask them permission for capturing opportunistic information in a passive, "authorize and forget" manner, they make sense as an element of the system if they fill significant information areas with reliable data that can be confronted and integrated with data already available.

The Crime Mapping System (point 4), the Security Dashboard (point 5) use the administrative data and offer different kinds of graphical and numerical representation. They can occasionally be developed starting from existing municipal Geographic Information Systems (GIS) and/or linked to databases and other tools that already provide synthetic tables of information. There is a multiplicity of possible software combinations that answer the needs of each specific context, including open source solutions. The same holds for statistical software packages and, ultimately, decisions should be based on compatibility with pre-existing infrastructures and instruments and with the specific characteristics and requirements of each local government.

The Software interface (point 6) is a technical need for the setting up of the system. As a matter of fact, it can be intended into two ways. On one hand, it is the container inside which all the queries are executed, the datasets connected, and the computations done using the dedicated tools and packages. On the other hand, it is the tool which gives the output to the final user in an interactive and easy to use interface. In fact, the final goal of a Smart Security system is to assist the Public Administrators and law enforcement agencies to understand a fast changing world and to implement the most effective security policies. The software system is the environment inside which the automated procedures defined by the experts are repeated automatically without the need of the final users to possess advance competences of statistics, video analysis, or software engineering. Obviously, given the sensitive nature of the data, security and control over the system and the information in it is crucial.

Table 2 gives a general overview of what we discussed in this final section and outlines what is needed for each component of a Smart Security. Starting from what we indicate in Table 2, any Municipality or Law enforcement agency can find its own roadmap towards a Smart Security System. Note that the Warning

Table 2 Requirements table for the key elements of a Smart Security System

Element of the Smart Security System	Requirements						
	Administrative database	Sensor network	Crime mapping	Security dashboard	Intelligence module: statistical analysis	Intelligence module: sensors analysis	Intelligence module: data integration
Crime mapping	Yes	No		No	No	No	Yes
Security dashboard	Yes	No	No		No	No	Yes
Statistical analysis module	Yes	No	Yes	Yes		No	Yes
Sensor analysis module	No	Yes	No	No	No		Yes

System is not listed in Table 2, being a very advanced feature of the system has various requirement as it must be tailored on the specific needs of the users.

Finally, intelligent solutions are ways to optimize the capacity, efficiency, and sustainability of a system. Typically, by means of ICT-based information processing. Smart technology is not, in itself, enough for a smart solution if users and operators are not involved in a learning process and the institutions that will use the system need to be changed as well. The system design should not focus on the smart infrastructure alone and not only on the final goal, but rather the transition phase itself should be designed carefully, with much attention for intermediate and hybrid stages where sometimes the flexibility gained from the intelligent solution can already be put to use [11].

References

1. Nam, T., & Pardo, T. A. (2011). Smart city as urban innovation: Focusing on management, policy, and context. In *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance* (pp. 185–194).
2. Harrison, C., & Donnelly, I. (2011). A theory of smart cities. In: *Proceedings of the 55th Annual Meeting of the International Society for the Systems Sciences (ISSS)*, *Hull* (Vol. 55, pp. 1–15).
3. Van den Berg, L., Pol, P. M. J, Mingardo, G., & Speller, C. J. M. (Eds.) (2006). *The safe city: Safety and urban development in European cities*. Farnham: Ashgate Publishing.
4. Weisburd, D., & McEwen, T. (1998). *Crime mapping and crime prevention*. New York: Criminal Justice Press.
5. Weisburd, D., Mastrofski, S. D., Greenspan, R., & Willis, J. J. (2004). *Growth of Compstat in American policing*. US Department of Justice: National Institute of Justice.
6. Steden, R., Boutellier, H., Scholte, R. D., & Heijnen, M. (2012). Beyond crime statistics: The construction and application of a criminogenity monitor in Amsterdam. *European Journal on Criminal Policy and Research, 19*, 47–62.
7. Bonatsos, A., Middleton, L., Melas, P., & Sabeur, Z. (2013). Crime open data aggregation and management for the design of safer spaces in urban environments. In *Environmental Software Systems. Fotering information Sharing* (pp. 311–320). Berlin, Heidelberg: Springer.
8. Bettencourt, L. (2013). The uses of big data in cities. Santa Fe Institute Working Paper 29.
9. Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., et al. (2012). Smart cities of the future. *European Physical Journal: Special Topics, 214*(1), 481–518.
10. Paskaleva, K. A. (2011). The smart city: A nexus for open innovation? *Intelligent Buildings International, 3*(3), 153–171.
11. De Haan, J., Vrancken, J. L. M., & Lukszo, Z. (2011). Why is intelligent technology alone not an intelligent solution? *Futures, 43*(9), 970–978.
12. Denzin, N. K. (2006). *Sociological methods: A sourcebook*. Piscataway: Aldine Transactions.
13. Paulsen, D. J., & Robinson, M. B. (2009). *Crime mapping and spatial aspects of crime*. Boston: Allyn & Bacon.
14. Chamlin, M. B., & Cochran, J. K. (2004). An excursus on the population size-crime relationship. *Western Criminology Review, 5*(2), 119–130.
15. Andresen, M. A. (2007). Location quotients, ambient populations, and the spatial analysis of crime in Vancouver, Canada. *Environment and Planning A, 39*(10), 2423–2444.

16. Andresen, M. A. (2006). Crime measures and the spatial analysis of criminal activity. *British Journal of Criminology, 46*(2), 258–285.
17. Boggs, S. L. (1965). Urban crime patterns. *American Sociological Review, 30*(6), 899–908.
18. Cohen, L. E., Kaufman, R. L., & Gottfredson, M. R. (1985). Risk-based crime statistics: A forecasting comparison for burglary and auto theft. *Journal of Criminal Justice, 13*(5), 445–457.
19. Harries, K. D. (1991). Alternative denominators in conventional crime rates. In: P. Brantingham & P. Brantingham (Eds.), *Environmental criminology* (2nd ed., pp. 147–165). USA: Waveland Press.
20. Harries, K. D. (2006). Property crimes and violence in United States: an analysis of the influence of population density. *International Journal of Criminal Justice Sciences, 1*(2), 24–34.
21. Sparks, R. F. (1981). Measuring crime rates and opportunities for crime. In: R.G. Lehnen & W. G. Skogan (Eds.), *The national crime survey: Working papers volume I: current and historical perspectives* (Vol. 1, pp. 52–58). Washington, DC: U.S. Department of Justice.
22. Stipak, B. (1988). Alternatives to population-based crime rates. *International Journal of Comparative and Applied Criminal Justice, 12*(2), 247–260.
23. Zhang, H., & Peterson, M. (2007). A spatial analysis of neighborhood crime in Omaha, Nebraska using alternative measures of crime rates. Internet Journal of Criminology. http://www.internetjournalofcriminology.com/Zhang%20Peterson%20-%20A%20SPATIAL%20ANALYSIS%20OF%20NEIGHBOURHOOD%20CRIME.pdf.
24. Thomas, W. I. (1966). Social disorganization and social reorganization. In M. Janovitz (Ed.), *On social organization and social personality: Selected papers* (pp. 3–11). Chicago: The University of Chicago Press.
25. Guerry, A. M. (1833). *Essai sur la statistique morale de la France*. Cochard.
26. Jacobs, J. (1961). *The death and life of great american cities*. New York: Vintage.
27. Newman, O. (1972). *Defensible space: Crime prevention trough urban design*. New York: MacMillan.
28. Jeffery, C. (1971). *Crime prevention through environmental design*. Thousand Oaks: Sage Publishing.
29. Clarke, R. V. G. (1997). *Situational crime prevention*. New York: Criminal Justice Press.
30. Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. In M. Tonry & N. Morris (Eds.), *Crime and justice: an annual review of research* (pp. Vol. 14, pp. 225–256). Chicago: The Chicago University Press.
31. Clarke, R. V. G. (1992). *Situational crime prevention: Successful case studies*. New York: Harrow and Heston.
32. Clarke, R. V. (1995). Situational crime prevention. In M. Tonry & D. Farrington (Eds.), *Building a safer society: Strategic approaches to crime prevention. Crime and justice: A review of research* (Vol. 19, pp. 91–150). Chicago: The Chicago University Press.
33. Felson, M., & Clarke, R. V. (1998). *Opportunity makes the thief: Practical theory for crime prevention*. London: Police and Reducing Crime Unit; Research, Development and Statistics Directorate. Police Research Series Paper 98.
34. Hillier, B. (1988). Against enclosure. In N. Teymur, T. A. Markus, & T. Woolley (Eds.), *Rehumanizing housing* (pp. 63–88). London: Butterworths.
35. Hillier, B., & Hanson, J. (1984). *The social logic of space*. Cambridge: Cambridge University Press.
36. Hillier, B., & Sahbaz, O. (2008). An evidence based approach to crime and urban design. In: R. Cooper, C. Boyko, G. Evans, & M. Adams (Eds.), *Designing sustainable cities: Decision-making tools and resources for design* (pp. 163–186). London: Wiley-Blackwell.
37. Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications*. Cambridge: Cambridge University Press.
38. Beavon, D. J. K., Brantingham, P. L., & Brantingham, P. J. (1994). The influence of street networks on the patterning of property offences. In R. V. Clarke (Ed.), *Crime prevention studies* (Vol. 2). New York: Willow Tree Press.
39. Cohen, L., & Felson, M. (1979). Social change and crime rates. *American Sociological Review, 44*, 588–608.

40. Eck, J. E., & Weisburd, D. (1995). Crime places in crime theory. In J. E. Eck & D. Weisburd (Eds.), *Crime and place*. Monsey.
41. Roncek, D. W. (1981). Dangerous places: Crime and residential environment. *Social Forces, 60*, 74–96.
42. Rice, K. J., & Smith, W. R. (2002). Socioecological models of automotive theft: Integrating routine activity and social disorganization approaches. *Journal of Research in Crime and Delinquency, 39*, 304–336.
43. Block, R., & Davis, S. (1996). The environs of rapid transit stations: A focus for street crime or just another risky place? In R. Clarke (Ed.), *Preventing mass transit crime*. New York: Criminal Justice Press.
44. Chih-Feng Shu, S. (2000). Housing layout and crime vulnerability. *Urban Design International, 5*(3–4), 177–188.
45. Hillier, B. (2004). Can streets be made safe? *Urban Design International, 9*(1), 31–45.
46. Sinkiene, J., Stankeviče, I., & Navickaite, K. (2012). Creating safer cities through urban planning and development. *Public Policy and Administration, 11*(3), 390–403.
47. di Bella, E., Persico, L., & Corsi, M. (2011). A multivariate analysis of the space syntax out-put for the definition of strata in street security surveys. In *DISEFIN Series of Economic Working Papers 5*.
48. Piquero, A. R., & Weisburd, D. (Eds.). (2010). *Handbook of quantitative criminology*. Berlin: Springer.
49. Schaffers, H., Komninos, N., & Pallot, M. (2012). Smart cities as innovation ecosystems sustained by the future internet. In *FIREBALL Project White Paper. EU* (pp. 1–65).
50. Yovanof, G. S., & Hazapis, G. N. (2009). An architectural framework and enabling wireless technologies for digital cities & intelligent urban environments. *Wireless Personal Communications, 49*, 445–463.
51. Farrington, D. P., Gill, M., Waples, S. J., & Argomaniz, J. (2007). The effects of closed-circuit television on crime: Meta-analysis of an English national quasi-experimental multi-site evaluation. *Journal of Experimental Criminology, 3*(1), 21–38.
52. Ratcliffe, J. H., Taniguchi, T., & Taylor, R. B. (2009). The crime reduction effects of public CCTV cameras: A multi-method spatial approach. *Justice Quarterly, 26*(4), 746–770.
53. Welsh, B. C., & Farrington, D. P. (2003). Effects of closed-circuit television on crime. *Annals of the American Academy of Political and Social Science, 587*, 110–135.
54. Welsh, B. C., & Farrington, D. P. (2005). Evidence-based crime prevention: Conclusions and directions for a safer society. *Canadian Journal of Criminology and Criminal Justice, 47*(2), 337–354.
55. Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly, 26*(4), 716–745.
56. Welsh, B. C., Mudge, M. E., & Farrington, D. P. (2010). Reconceptualizing public area surveillance and crime prevention: Security guards, place managers and defensible space. *Security Journal, 23*(4), 299–319.
57. Remagnino, P., Monekosso, D. N., & Jain, L. C. (2011). *Innovations in defence support systems—3: Intelligent paradigms in security*. Berlin: Springer.
58. van den Hengel, A., Hill, R., Wart, B., Cichowski, A., Detmold, H., Madden, C., Dick, A., & Bastian, J. (2009). Automatic camera placement for large scale surveillance networks. In *Workshop on Applications of Computer Vision*.
59. Zini, L., Cavallaro, A., & Odone, F. (2013). Action-based multi-camera synchronization. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 3*(2), 165–174.
60. Haritaoglu, I., Harwood, D., & Davis, L. (2000). W4: real-time surveillance of people and their activities. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 22*(8), 809–830.
61. Khan, B. S., & Shah, M. (2003). Consistent labeling of tracked objects in multiple cameras with overlapping fields of view. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 25*(10), 1355–1360.
62. Taj, M., & Cavallaro, A. (2011). Distributed and decentralized multi-camera tracking: A survey. *IEEE Signal Processing Magazine, 28*(3), 46–58.

63. Gheissari, N., Sebastian, T., & Hartley, R. (2006). Person re-identification using spatiotemporal appearance. In *IEEE Conference on Computer Vision and Pattern Recognition* (pp. 1528–1535).
64. Zheng, W., Gong, S., & Xiang, T. (2011). Person re-identification by probabilistic relative distance comparison. In *IEEE Conference on Computer Vision and Pattern Recognition* (pp. 649–656).
65. Stan, L., & Jain, A. (2011). *Handbook of face recognition*. Berlin: Springer.
66. Shachtman, N. (2006, January 25). The new security: cameras that never forget your face. *The New York Times*, Published.
67. Viola, P., & Jones, M. (2004). Robust real-time face detection. *International Journal of Computer Vision, 57*(2), 137–154.
68. Poppe, R. (2010). A survey on vision-based action recognition. *Image and Vision Computing, 28*(6), 976–990.
69. Bird, N., Masoud, O., Papanikolopoulos, N., & Isaacs, A. (2005). Detection of loitering individuals in public transport areas. *IEEE Transactions on Intelligent Transportation Systems, 6*(2), 167–177.
70. Krausz, B., & Bauckhage, C. (2011). Automatic detection of dangerous motion behavior in human crowds. In *IEEE International Conference on Advanced Video and Signal-based Surveillance, AVSS*.
71. Stauffer, C., Eric, W., & Grimson, L. (2000). Learning patterns of activity using real-time tracking. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 22*(8), 747–757.
72. Atev, S., Masoud, O., & Papanikolopoulos, N. (2006). Learning traffic patterns at intersections by spectral clustering of motion trajectories. In *IROS Intelligent Robots and Systems* (pp. 4851–4856).
73. Morris, B. T., & Trivedi, M. M. (2008). A survey of vision-based trajectory learning and analysis for surveillance. *IEEE Transactions on Circuits and Systems for Video Technology, 18*(8), 1114–1127.
74. Noceti, N., & Odone, F. (2012). Learning common behaviors from large sets of unlabeled temporal series. *Image and Vision Computing, 30*(11), 875–895.
75. Estellés-Arolas, E., & González-Ladrón-De-Guevara, F. (2012). Towards an integrated crowdsourcing definition. *Journal of Information Science, 38*, 189–200.
76. Cuff, D., Hansen, M., & Kang, J. (2008). Urban sensing: Out of the woods. In *Communications of the ACM*, Vol. 51.
77. Ganti, R. K., Ye, F., & Lei, H. (2011). Mobile crowdsensing: Current state and future challenges. In *IEEE Communications Magazine* (pp. 32–39).
78. Cardone, G., & Foschini, L. (2013). Fostering participation in smart cities: A geo-social crowdsensing platform. *IEEE Communications Magazine, 51*(6), 112–119.
79. Coric, V. & Gruteser, M. (2013). Crowdsensing maps of on-street parking spaces. In *2013 IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)* (pp. 115–122).
80. Ghose, A., Bhaumik, C., & Chakravarty, T. (2013). BlueEye: A system for proximity detection using bluetooth on mobile phones. In *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication* (pp. 1135–1142).
81. Heipke, C. (2010). Crowdsourcing geospatial data. *ISPRS Journal of Photogrammetry and Remote Sensing, 65*, 550–557.
82. Kumagai, J., & Cherry, S. (2004). Sensors and sensibility. *IEEE Spectrum, 41*(7), 22–28.
83. The Constitution Project. (2006). Guidelines for public video surveillance, a guide to protecting communities and preserving civil liberties.
84. Newton, E. M., Sweeney, L., & Malin, B. (2005). Preserving privacy by de-identifying face images. *IEEE Transactions on Knowledge and Data Engineering, 17*(2), 232–243.
85. Cavallaro, A. (2004). Adding privacy constraints to video-based applications. In *European Workshop on the Integration of Knowledge, Semantics and Digital Media Technology*.
86. Dufour, J. Y. (Ed.) (2012). *Intelligent video surveillance systems*. London: Wiley.
87. Block, C. (1998). The geoArchive: An information foundation for community policing. In *Crime Mapping and Crime Prevention* (pp. 27–81).

88. Buslik, M., & Maltz, M. (1998). Power to the people: Mapping and information sharing in the Chicago Police Department. In *Crime Mapping and Crime Prevention, Crime Prevention Studies* (Vol. 8).
89. Cohen, J., Gorr, W., & Olligschlaeger, A. (2007). Leading indicators and spatial interactions: A crime forecasting model for proactive police deployment. *Geographical Analysis, 39*(1), 105–127.
90. Cohen, J., & Gorr, W. (2005). *Development of crime forecasting and mapping systems for use by police*. Pittsburgh: H. John Heinz III School of Public Policy and Management, Carnegie Mellon University.
91. Cocx, T. K., Kosters, W. A., & Laros, J. F. J. (2008). *An Early Warning System for the Prediction of Criminal Careers. MICAI 2008: Advances in Artificial Intelligence* (pp. 77–89). Berlin, Heidelberg: Springer.
92. Andersen, J. J. (2013). Assess the urban surveillance infrastructure: Develop a framework. In *IBM Development* (pp. 1–11).
93. Rezaei, A., Rossi, B., Sillitti, A., & Succi, G. (2012). Knowledge extraction from events flows. In G. Anastasi, E. Bellini, E. Di Nitto, C. Ghezzi, L. Tanca, & E. Zimeo (Eds.), *Methodologies and technologies for networked enterprises*. Berlin: Springer.
94. Kimball, R., & Ross, M. (2013). *The data warehouse toolkit: The definitive guide to dimensional modeling*. London: Wiley.
95. NoSQL Archive. http://nosql-database.org/.
96. Predonzani, P., Sillitti, A., & Vernazza, T. (2001). Components and data-flow applied to the integration of web services. In *IEEE Conference on Industrial Electronics Society* (Vol. 3, pp. 2204–2207).
97. Semantic Web. http://semanticweb.org/.
98. Scotto, M., Sillitti, A., Vernazza, T., & Succi, G. (2001). Managing web-based information. In *5th International Conference on Enterprise Information Systems* (Vol. 1, pp. 575–578).
99. Sillitti, A., Scotto, M., Succi, G., & Vernazza, T. (2003). News miner: A tool for information retrieval. In *7th International Conference on Intelligent Engineering Systems*.
100. W3C Standards Semantic Web. http://www.w3.org/standards/semanticweb/ontology.
101. Moore, M. H., & Aa, Braga. (2003). Measuring and improving police performance: The lessons of Compstat and its progeny. *Policing: An International Journal of Police Strategies & Management, 26*, 439–453.
102. Weisburd, D., Mastrofski, S. D., Greenspan, R., & Willis, J. J. (2004). *The growth of compstat in American policing*. Washington, DC: Police Foundation.
103. Chainey, S., & Ratcliffe, J. (2008). *GIS and crime mapping*. London: Wiley.
104. Harris, K. D. (1999). *Mapping crime: principles and practice*. Washington, DC: U.S. Department of Justice.
105. Kennedy, L. W., Caplan, J. M., & Piza, E. (2010). Risk clusters, hotspots, and spatial intelligence: Risk terrain modeling as an algorithm for police resource allocation strategies. *Journal of Quantitate Criminology, 27*, 339–362.
106. Groff, E., Fleury, J., & Stoe, D. (2001). *Strategic approaches to community safety initiative (SACSI): Enhancing the analytic capacity of a local problem-solving effort*. Washington, DC: National Institute of Justice.
107. Pattavina, A., Pierce, G., & Saiz, A. (2002). Urban neighborhood information systems: crime prevention and control applications. *Journal of Urban Technology, 9*, 37–41.
108. Roehl, J., Rosenbaum, D. P., Costello, S. K., Coldren, J. R, Jr, Schuck, A. M., Kunard, L., et al. (2008). *Brief paving the way for project safe neighborhoods: SACSI in 10 US cities*. Washington, DC: U.S Department of Justice.
109. Boba, R. (2009). *Crime analysis with crime mapping*. Beverley Hills: Sage Publications.
110. Monahan, T., & Mokos, T. J. (2013). Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. *Geoforum, 49*, 279–288.
111. Lee, J., & Yu, C. (2010). The development of Urban Crime Simulator. In *Proceedings of the 1st International Conference and Exhibition on Computing for Geospatial Research & Application—COM.Geo'10* (p. 1). New York, USA: ACM Press.