"BABEȘ-BOLYAI" UNIVERSITY CLUJ-NAPOCA
DOCTORAL SCHOOL OF INTERNATIONAL RELATIONS
AND SECURITY STUDIES
FACULTY OF HISTORY AND PHILOSOPHY
Domain: International Relations and European Studies

PH.D. THESIS

- SUMMARY -

Scientific coordinator:
Professor Ph.D. Adrian Liviu Ivan

Ph.D. Candidate:
Jr. Ing. Rareș-George Codrean

Cluj-Napoca
2021

"BABEŞ-BOLYAI" UNIVERSITY CLUJ-NAPOCA
DOCTORAL SCHOOL OF INTERNATIONAL RELATIONS
AND SECURITY STUDIES
FACULTY OF HISTORY AND PHILOSOPHY
Domain: International Relations and European Studies

SAFE CITY IN THE CONTEXT OF THE TERRORIST THREATS AND CRIME IN THE EUROPEAN UNION. CASE STUDY: ORADEA MUNICIPALITY

Scientific coordinator:
Professor Ph.D. Adrian Liviu Ivan

Ph.D. Candidate:
Jr. Ing. Rareş-George Codrean

Cluj-Napoca
2021

CONTENTS

KEY-WORDS: safecity, smartcity, public order, security, technical security systems

I. INTRODUCTION

The public administration authorities were created for a noble purpose, namely the PROTECTION OF THE CITIZEN. These are the elements responsible for the safety of the citizens, of the community as a whole against those who defy the rules of the state of law.

The cyber revolution is considered *the most important global transformation since the beginning of the industrial revolution*. (Gershwin, L. K., 2015).

The topic chosen to be deepened in the doctoral research is: **SAFE CITY IN THE CONTEXT OF THE TERRORIST THREATS AND CRIME IN THE EUROPEAN UNION. CASE STUDY: ORADEA MUNICIPALITY**, which aims to address the problem of the implementation of the technical security systems, monitoring and analysis, their synchronization through secure communication in cyberspace and the centralization of all field information in a central dispatcher to be monitored, archived and used accordingly, so that the decision-making power to be based on true information at the critical moments or on the development of security and public order strategies.

First of all, we must mention the fact that Safe City is not a product and it is not a service. Safe City is a complex system created by the central and local public authorities together with the citizens of the community, of the academic environment and tof he private business environment - which comes with know-how, technologies and products to be implemented in an interconnected system. In order to define a city as being *smart and sustainable*, it must use technology, electronic data collection sensors, automation systems and encrypted, secure communication, with the aim of improving the quality of life, automation and efficiency of urban services and their interconnection, ensuring the present and future needs regarding the aspects of the social, economic and environmental security. (Dumitrașcu, E., 2018).

Statistically, in the last ten years, in Romania there is clearly a major discrepancy between the localities that manage the safety and public order issues only with the human factor (where the degree of aggression of some groups has increased, safety in public space has decreased, and the number of road accidents and, as well, the number of thefts and robberies reach alarming levels) and localities where the human factor is aided by the civil security technology, and the human factor is used at its true value, namely for monitoring and data analysis. Technology is used to gather information, being a much better means of proof, omnipresent and with a flawless memory. In these localities, statistically, from one year to another the security and public order incidents decrease exponentially, reaching in 2015 values below 50% compared to 2005. (INSSE, 2015)

We will seek to streamline the general framework for organizing the operation of the security and public order system both in terms of utility and financial efficiency. We will reduce the number of human personnel in the field, they will be improved in the analysis of information and decision making, and the collection of the information will be done with human personnel only in exceptional situations (we estimate 20% of cases).

We exemplify here in roder to highlight the importance: The economic district of London, Canary Wharf, is one of the points with the highest degree of security on the planet. In Canary Wharf, security and public order are managed by a private company (Richard George, Rob I. Mawby, 2015), and 90% of the information is collected with a technical monitoring systems. The London police monitors, analyzes and administers all information from the central dispatchers and intervenes only in exceptional cases. Canary Wharf is a model of Safe City Systems for all major cities in the world. The Safe City system in Canary Wharf is close to the ideal system, both in terms of efficiency and in terms of implementation, administration and use costs. Let's do a quick calculation: what is the cost of operating a system of 10 surveillance cameras for 5 years (the amortization time of an electronic device) connected to an image analysis software capable of automatically detecting traffic violations, an abandoned luggage, the use of a weapon or even the breaking of a window and burglary and what is the cost of maintaining a permanent monitoring post with human personnel (police, local police, gendarmerie, or any other structure in the field of public order) for 5 years? We mention the fact that for a job of 24/24 you need at least 4 employees. Also, let's try to analyze what is more effective in gathering the incriminating evidence in real time: a law enforcement officer or 10 surveillance cameras connected to the analysis software described above?

Of course, the intervention and detention of the offender can be done only with human personnel able to think of the exceptional measures necessary in such cases. But we can greatly reduce the costs of gathering information, so that the human personnel are specialized and used only in the advanced stages of the incident.

According to the specifics of all the scientific systems, the information system is based on certain basic notions that allow the further development and refinement of the system. The primary notion of the information system is, intuitively, the information (Collin. S, M.H., 1990) (Beyon, D., 1990), (Luckey, T., 1991); An alternative to this premise is to treat the data as a primary notion (ACCA, 1988), (Watters, C., 1992). If the basic unit is the information, the notion of data is treated as a derivative, whereas if the basic unit is data, the information is considered as a derivative of the date. We will approach first the notion of the information, and later the data.

The research methodology chosen to study the issue of information security is that of the case study. This method was chosen taking into account the inherent complexity of the issue, but also the limited control of the contemporary institutions and structures, both public and private, over public safety and order. The realization of a case study allows the interrogation of the current modalities of computer security, but also the investigation of some possibilities for the improvement of the system. This research method allows us to gradually approach the investigated issues, by incrementally treating the empirical support. The primary variable of our study is: *The need to modernize the architecture of the Safe City systems, of the working procedures, of the priorities and of the system of participation and distribution of the resources available to bodies and institutions directly or indirectly involved in the operation of these systems.* The secondary variable is: *The modernization of the architecture of the current Safe City type systems and the policies on the implementation, monitoring and use of these systems must provide the decision-making power with a true information base, both to maintain the general security and public order,*

and to manage the critical moments, and for the development of new security and public order strategies.

To carry out the empirical study, the research plan is built for the transition from the primary variable to the secondary variable. The empirical data will be manipulated to answer the initial research questions. The manipulation will be done by analyzing the data, and the results of the analysis will generate a series of conclusions regarding the initial questions (Yin, 2005).

The analysis of the issues proposed for research will be interdisciplinary, based on three main fields of study: technology for civilian public security, state bodies responsible for security and public order and their interoperability, but also cyber security, communications security and digital information security, private or classified.

For these reasons, we consider that the subject of the doctoral thesis *SAFE CITY IN THE CONTEXT OF THE TERRORIST THREATS AND CRIME IN THE EUROPEAN UNION. CASE STUDY: ORADEA MUNICIPALITY* it is very opportune, topical and with very high chances of practical application.

II. RESEARCH METHOD

The research method used to carry out this work is that of the case study, as theorized by Yin (Yin, 2005). This research method is ideal for approaching explanatory questions such as *why* and *how*. The phenomenon studied is the need to modernize the architecture of the Safe City systems, working procedures, priorities and the system of participation and sharing of resources for bodies and institutions directly or indirectly involved in the implementation, monitoring and use of these systems. The aim of the research is to demonstrate that modernizing the architecture of the Safe City systems and policies for their implementation, monitoring and use can provide decision-makers with access to superior information bases, which can improve both the day-to-day security and crisis management, and can provide the necessary premises for the development of new public order management strategies.

This method is used to reveal the necessary conditions for the efficient and substantial modernization of the architecture of the Safe City systems, including the procedures related to their operationalization, but also the systems of participation and distribution of resources for institutional actors directly or indirectly involved in the implementation, monitoring and use of these systems. The case study will highlight the major points of interest, highlighting the aspects in which the modernization can have a major impact in improving the Safe City systems. Moreover, this method will also make it possible to distinguish aspects that are already functional and do not require intervention. In order to avoid the trap of relying on the appearances, we will collect empirical data on the operation of the Safe City systems, and these data will be analyzed according to the methodology.

The research pattern is composed of the following elements:

II.1. What questions do we need to answer?

The presentation of the research questions is the first component of the research pattern. The research questions are of critical importance to the research as a whole, as they outline the boundaries of the research, delimiting its subject. At the same time, the research questions play a critical role in choosing the research methodology, because each type of question requires a

specific analysis and the collection of a certain type of data. In this sense, the questions like *how* and *why* are of an explanatory nature, requesting the involvement in the case study of some data on the operationalization of the studied systems, but also on the reasons why these systems were structured in the manner contemporary. Consequently, these questions challenge us to investigate more than the simple components of the Safe City systems, requiring an analysis of the operational links between the elements studied, but also of the reasons why the operational links were made in this way.

In accordance with the requirements of the type of questions chosen - namely "how" and "why" - In order to investigate the need to modernize the Safe City systems, it is necessary to use a case study that allows a detailed analysis of some data on the procedures for operationalizing Safe City systems, their priorities, but also the participation systems of the institutions involved and the distribution of information resources between these institutions.

After clarifying the nature of the chosen research questions, it is necessary to specify them and specify the order in which they are analyzed. In this regard, the research questions addressed in this study are the following:

1. How and why is it necessary to modernize the architecture of the Safe City systems, working procedures, priorities and a system of participation and sharing of resources for bodies and institutions directly or indirectly involved in the implementation, monitoring and use of this system?

2. How is improved the architecture of the current Safe City systems and policies on the implementation, monitoring and use of these systems to ensure the decision-making power a true information base, both for maintaining security and public order, but also in critical moments or at the development of security and public order strategies?

3. Why is the modernization of the current Safe City type systems and the policies regarding the implementation, monitoring and use of these systems to ensure the decision-making power a true information base, both for maintaining security and public order, but also in the moments critical or to the development of security and public order strategies?

II.2. Establishing the working hypothesis

The second component of the research pattern is the research hypothesis. The research hypothesis is the stage in which we announce the premise of the research project, mentioning what is the result that we expect our project to produce. In this sense, the research hypothesis must capture the initial position on the issue addressed. The purpose of our case study is to test the hypothesis by analyzing the empirical data, which will either invalidate or confirm the chosen hypothesis.

Given that our case study focuses on the architecture of the Safe City systems, the hypothesis must announce a position on the nature of this architecture. The purpose of our case study is not limited to an overview of the status quo of these systems, but seeks to discover the key points that need to be addressed to improve the functioning of the Safe City systems. Consequently, we chose as points of interest of our study the working procedures, priorities and the system of participation and sharing of resources for the bodies involved in the implementation, monitoring

and use of this system. These points of interest have been chosen because they are fundamental components of the Safe City systems, and their analysis can provide us with informed conclusions about the possibilities for improving these systems.

Our case study starts from the need to modernize the Safe City systems in order to improve their functioning, by virtue of achieving the ultimate goal of ensuring a greater protection of the citizens, both in everyday life and, especially, in the context of crisis situations. In this sense, our hypothesis does not aim to establish the need for the modernization of the Safe City systems, as the need for modernization is confirmed by the existence of clear syncopes in these systems, which make possible the criminal or terrorist events of recent years. Consequently, our hypothesis aims at identifying those aspects of the Safe City type system in which the intervention is a necessary one in such a way that the modernization is an efficient one, which would produce a palpable impact in the life of the citizens.

The established hypothesis is the following: **If it is necessary to modernize the architecture of the Safe City systems, and the existing governance related to their use, then must be modernized the architecture of the current Safe City systems and policies on the implementation, monitoring and use of these systems, to ensure decision-making powers, a basis of true information, both for maintaining the state of security and public order, but also in critical moments or în case of the development of security and public order strategies.**

II.3. Analysis of primary, contextual and global units

The analysis of the primary, contextual and global units represents the third component of the research pattern and refers to the fundamental problem of defining *the case*. In our case we cannot refer to systems or groups of systems but to a *complex* technical, social, economic and administrative *phenomenon* which is represented by the need to modernize the architecture of the Safe City systems: working procedures, priorities and a system of participation and sharing of resources for the bodies and institutions directly or indirectly involved in the implementation, monitoring and use of this system, but also in an entity - the Central County Monitoring Dispatch Office -, elements not so easy to define as a fully integrated system.

The correct identification of the units of analysis is a fundamental stage of the research methodology, as it allows us to focus the case study on the fundamental aspects on which our research can provide us with information that confirms our hypothesis and helps us answer in a synthetic way at the research questions. Given that our case study does not focus on static objects, which can be studied in isolation from the systems to which they belong, but on operational and decision-making processes that are interdependent, the definition of units of analysis is a delicate one. We risk, on the one hand, choosing as units of analysis too isolated aspects of these processes, which could obstruct our ability to draw correct conclusions about the overall functioning of these systems. The second trap we must avoid is to choose as units of analysis too broad aspects of the Safe City systems, which would prevent us from being able to accurately identify the key points where we need to intervene to ensure the efficient modernization of these systems.

To avoid these traps, we will apply the methodology provided by Yin: *a) variations in the definition of decisions, programs, implementation processes or organizational changes, and b) their components that already existed before their formal nomination* (Yin, 2005). Consequently, we must first identify the variations that may occur in defining the elements we will study during our research, so as to ensure that we maintain the same units of analysis throughout the study, in order to ensure the coherence of the case study. At the same time, we must keep in mind that any

attempt to define the units of analysis is a subdivision of processes that are in fact continuous and interdependent, and this subdivision must be made given the overall operation of these systems.

The analysis unit of our study is the architecture of *the Safe City systems, working procedures, priorities and a system of participation and sharing of resources for bodies and institutions directly or indirectly involved in the implementation, monitoring and use of this system.* However, it is necessary to specify that this unit of analysis is a flexible one, which may change during the study, depending on the preliminary results provided by the empirical data analyzed.

II.3.1. Primary unit

The primary unit is: **MODERNIZING THE ARCHITECTURE OF THE CURRENT SAFE CITY SYSTEMS AND POLICIES REGARDING THE IMPLEMENTATION, MONITORING AND USE OF THESE SYSTEMS IN A EUROPEAN CONTEXT**.

II.3.2. Contextual unit, the existence of the case

The contextual unit is the very existence of the case: **THE NEED TO MODERNIZE THE ARCHITECTURE OF THE SAFE CITY SYSTEMS AND WORK PROCEDURES, PRIORITIES AND A SYSTEM OF PARTICIPATION AND SHARING OF RESOURCES FOR BODIES AND INSTITUTIONS DIRECTLY OR INDIRECTLY INVOLVED IN THE IMPLEMENTATION, MONITORING AND USE OF THIS SYSTEM** .

II.3.3. Build-in unit

The buiklt-in unit is: the **MODERNIZATION OF THE ARCHITECTURE OF THE CURRENT SAFE CITY SYSTEMS THROUGH THE MANAGEMENT OF POLICIES REGARDING THE IMPLEMENTATION, MONITORING AND USE OF THESE SYSTEMS IN A EUROPEAN CONTEXT**.

II.3.5. According to what criteria are the data interpreted?

The fifth component of the research methodology is the establishment of criteria for the interpretation of the empirical data. Intuitively, the data can provide different conclusions, depending on how they are interpreted. The criteria for interpreting the data therefore function as a pair of lenses that filter the empirical material, modeling them according to the nature of the chosen criterion. The issue of choosing the interpretation criteria is even more acute in cases where there is no satisfactory overlap of the anticipated pattern with the pattern extracted from the empirical data. In this case, there is a need to re-evaluate the criteria, or to expand the data sample. However, our hypothesis is one that can be easily invalidated, using a series of connections between the modernization of some elements of the system (working procedures, priorities, and systems of participation and sharing of resources for the institutions involved) and the modernization of the overall architecture of the system. In this sense, we must keep in mind that the purpose of our research is not an intrinsic one, which serves only to other researches in the field, but is subordinated to the imperative practical need to improve the architecture of the Safe City systems to ultimately improve the degree of public safety.

We must keep in mind that the criteria for interpreting the data must take into account, on the one hand, the explanatory nature of our case study which aims to answer, in particular, the question "how" the architecture of the Safe City systems can be modernized, and, on the other hand, the need to identify in the patterns extracted from the data analysis the same link between the independent variable and the independent variables as in the anticipated pattern. The independent variable we operate with is the current architecture of the Safe City systems, and the dependent variables are the work procedures, priorities and systems for participation and sharing

of resources for the institutions involved in the Safe City systems. The aim of our research is to present a correlation between the modernization of the elements chosen as dependent variables, and the modernization of the overall systems, which constitute the independent variables.

The criteria used for the data analysis must meet the specific requirements of a scientific research, capable of generating the basis for effective interventions in the architecture of the Safe City systems. In this regard, we reiterate the use of objectively processed data, without choosing only the data that confirm the chosen hypothesis, and we are determined to explore alternative explanations, even if they have the potential to invalidate the hypothesis (Yin, 2005). Moreover, for the interpretation of data we use logical models, as they were defined by Yin: *The logical model intentionally stipulates a complex chain of events in time. These are included in repeated cause-effect-cause-effect patterns* (Yin, 2005).

The use of the logical model of cause-effect-cause-effect allows the establishment of causal relationships between the analyzed data. In this sense, the purpose of our case study is to identify causal patterns between the modernization of the working procedures, priorities, and the system of participation of the institutions and the modernization of the general architecture of the system. The use of causality as a criterion for interpreting data allows us to base our case study strictly on the causal relationships, and not on simple correlations that can be explained by alternative hypotheses. This criterion for interpreting the data is a very strict one, which is very difficult to satisfy. However, the advantage of using causality as a criterion for interpreting data is that it allows us to base our case study on evidence that cannot be invalidated by alternative explanations. Consequently, the result of our case study will have immediate practical applicability, as it will show us, by establishing causal relationships, which elements of the Safe City systems need to be upgraded to improve the overall architecture of the systems.

II.3.4. Correlation of the data with the hypothesis

The fourth component of the case study pattern is the linking of data to the research hypothesis. This component of the research methodology aims to adapt the available database to the requirements established by the hypothesis, so that the manipulation of the data allows the hypothesis to be invalidated or confirmed.

The linking of the hypothesis data can be done in a plurality of methods, but the most appropriate method for the case studies is the pattern matching, as theorized by Donald Campbell in 1975 (Yin, 2005, p. 143). The pattern matching technique involves comparing a pattern made using empirical data with the anticipated hypothesis pattern, but also with other possible alternative patterns, to avoid the trap of confirming the hypothesis without exploring alternative explanations (Trochim, 1989). The role played by the use of alternative explanations is a vital one, because it allows the final result to be a solid one and able to be translated into practice, and not a simple speculation in which are chosen from the databases exactly the data that confirm the hypothesis.

The anticipated pattern of the chosen hypothesis is that the modernization of the current architecture of the Safe City systems must aim at modernizing the working procedures, their priorities, but also the system of participation and sharing of resources for bodies and institutions directly and indirectly involved in the implementation, monitoring and the use of these systems. Accordingly, we will analyze the empirical data on the working procedures, priorities and ways of participation of the Safe City systems, in order to investigate whether their modernization causes a perceptible modernization of the overall architecture of these systems. If a significant change in the operational quality of the systems is perceived after the modernization of the components

mentioned above, then the anticipated pattern will be superimposed on the pattern extracted from the empirical data, which will lead to the confirmation of the case study hypothesis.

II.4. The theoretical part of the thesis

The previous sub-chapters introduced the components of the research methodology used in our case study. In this chapter, we will elaborate the preliminary theory on the approached topic, which will guide us in the first stages of the research.

The elaboration of the theoretical part of the thesis is a specific aspect of our methodology, of the case study. The alternative research methods, such as ethnographies, genealogies, or *grounded theories* do not require the formulation of hypotheses at the beginning of investigations (Yin 2005, p. 47). These methodologies avoid the inauguration of the research by formulating hypotheses, because they are based on the premise that the initial formulation of the hypotheses function as *lenses* that influence how the data is collected and processed, which undermines the objectivity of the analysis, resulting in affecting the final quality of the extracted conclusions. However, it is important to point out that these alternative methodologies also have specific disadvantages. Consequently, by avoiding the formulation of theoretical hypotheses, these methods immediately move to the stage of collecting field data, which leads to the collection of data masses that cannot be structured or filtered and which are often, in fact, irrelevant to the object studied. The operation with theoretical hypotheses facilitates the collection of the data, as it allows the identification of points of interest and, at the same time, the choice of methods by which the data will be interpreted later (in our case it is the case of the criterion of causality).

The development of preliminary theories is not only important for facilitating the data collection. Another essential role of the preliminary theories is to identify the level of generalization at which the study will be conducted. Therefore, according to Yin, the preliminary theories represent instances of *analytical generalization* (Yin, 2005, p. 51) through which is created a pattern with which to operate in the data collection stage. The analytical generalization must be understood in contrast to the statistical generalization, relevant to analyzes that operate with databases that can be converted into quantitative formulas (Yin, 2005, p.51). Unlike the statistical generalization, the analytical generalization allows us to formulate an initial pattern that we can contrast with the patterns identified by analyzing the empirical data. The preliminary theories are the support through which this analytical generalization is built, as they allow the identification of some initial positions that we will seek to confirm by comparing them with the analyzed data. We would like to remind, however, that our paperwork operates with a criterion of causality; therefore, our preliminary theory will only be confirmed if we can establish a causal relationship between the modernization of the components chosen as analytical units on the one hand, and the improved functioning of the overall architecture of the Safe City systems on the other.

It is vital to point out that for the case study method the elaboration of preliminary theories is a fundamental stage of the research methodology. We reiterate that the purpose of our case study is to establish a causal relationship between the modernization of some components of the Safe City systems and the modernization of the integral architecture of these systems. One of our preliminary theories is that the efficient modernization of the Safe City systems is to create the possibility of synchronizing security systems that are currently isolated through a secure communication platform in the cyber space. Moreover, it is necessary to establish a dispatcher to centralize all information taken over by the individual systems, so that this information provided

in real time can be monitored, archived and used by institutional actors involved in ensuring the security. This constantly retrieved information can provide public decision-makers, especially the local government apparatus, with the fundamental basis for adopting strategies to improve the public security. The centralized information can play a key role in revealing the weaknesses of the security systems, so that the systems can be optimized both for their day-to-day operations and, in particular, for the crisis management. Therefore, the preliminary theory of this case study is that the development of a centralized database in the cyberspace can produce a considerable improvement in security, both in ordinary situations and in crisis situations.

The elaboration of this theoretical part of the thesis offers us a standard through which we will be able to analyze the empirical data. The purpose of this theory is, therefore, to provide us with a mechanism through which we can operate with the empirical data in such a way that we can identify in the empirical support the data that confirm our hypothesis, but also those that invalidate it. In this sense, by appealing to our preliminary theory we will be able to filter the collected data. At the same time, we must keep in mind that the preliminary theory is a flexible standard, which can be adapted by contrasting it with the empirical material analyzed. Consequently, the preliminary theory does not work as an absolute filter through which we analyze the empirical material, but the relationship between the theory and the empirical data is a dual one: on the one hand, the preliminary theory helps us in collecting relevant data, but on the other hand, the data collected helps us to model and improve the preliminary theory in such a way that it can be modeled during the study to the form that satisfies the strictly established causal criterion.

We start the theorizing of **the primary unit of analysis**: **THE MODERNIZATION OF THE ARCHITECTURE OF THE CURRENT SAFE CITY SYSTEMS AND POLICIES REGARDING THE IMPLEMENTATION, MONITORING AND USE OF THESE SYSTEMS TO ENSURE THE DECISION-MAKING POWER A TRUE INFORMATION BASE, BOTH FOR MAINTAINING THE SECURITY AND THE PUBLIC ORDER, BUT ALSO IN CRITICAL MOMENTS OR IN DEVELOPING STRATEGIES FOR SECURITY AND PUBLIC ORDER.**

According to the National Strategy for Public Order 2010-2013, *the public order is the component of the national security, represented by the state of legality, balance and social peace, corresponding to a socially acceptable level of observance of the legal norms and civic conduct, which allows the exercise of rights and fundamental human freedoms, as well as the functioning of the structures specific to the rule of law and are characterized by the credibility of the institutions, the public health and morals, the state of normalcy in the organization and conduct of the political, social and economic life, in accordance with the legal, ethical, moral religious and other, generally accepted by society* (O.G. GD 196/2005, 2005).

At the same time, according to the National Strategy for Public Order 2010-2013, the public safety expresses the feeling of peace and trust, which the state institutions confer for the application of measures to maintain the public order and the tranquility, the degree of security of individuals, communities and property, as well as for the realization of the civil society-police partnership, in order to solve the problems of the community, to defend the rights, freedoms and legal interests of the citizens (O.G. GD 196/2005, 2005)

II.4.1. Organizations and institutions directly involved: Public order forces

The public order forces designate the institutions invested and entitled to exercise the right of police. Specifically, they are those authorities and institutions that have attributions and

competences in the field of security and public order and have the right to summon any individual in order to comply with the law and the rules of conduct violated.

    A. Specialized forces
    B. Complementary forces
    C. Exceptional forces for the defense of public order
    D. Organizations and institutions indirectly involved

II.4.2. State of affairs
II.4.2.1. The current crime situation in Oradea Municipalty, Bihor County and the North-West Region of Romania
II.4.2.1.A. Human trafficking
II.4.2.1.B. Drug trafficking
II.4.2.1.C. Cyber Crime
II.4.2.2. The current terrorist threats in Oradea and regions

Next we will theorize the **contextual unit**, this being the very existence of the case: **THE NEED TO MODERNIZE THE ARCHITECTURE OF THE SAFE CITY SYSTEMS AND POLICIES ON THE IMPLEMENTATION, MONITORING AND USE OF THESE SYSTEMS IN ORDER TO ENSURE THE DECISIVE POWER OF A TRUE INFORMATION BASE, BOTH FOR MAINTAINING THE SECURITY AND PUBLIC ORDER, BUT ALSO IN CRITICAL MOMENTS OR IN THE DEVELOPMENT OF SECURITY AND PUBLIC ORDER STRATEGIES**. In the first part we will conceptualize the need to modernize the current architecture of the Safe City systems, and in the second we will analyze the working procedures, priorities and a system of participation and sharing of resources for bodies and institutions directly or indirectly involved in the implementation, monitoring and the use of this system.

The analysis of the systems implemented so far in Romania reveals an incipient stage of the preoccupation of the territorial administrative structures towards this field. However, I believe that although they face major problems related to the underfunding of the field, the Safe City systems must become a priority for the decision makers of the territorial administrative structures in Romania. We support this statement based on the calculations and statistics both in terms of efficiency and in terms of costs in the medium and long term, by comparing the implementation of a Safe City system with maintaining the security and public order policies based only on the human factor.

In the Case Study we will also address topics that have not been addressed before in the Romanian literature, such as the interoperability of the security agencies in the use and decision-making based on the use of the Safe City systems, an activity used in this moment like"firefighting", chaotic, because no study has been carried out to create framework policies and processes for the use of the centralized Safe City monitoring systems by defense and public order bodies.

We will show why the implementation, monitoring and, moreover, the entire management of the Safe City Systems succeeded only when the architecture was thought from the very beginning as being an integrated system, at least at locality level or, ideally, at county level.

We are going to theorize the **built-in analysis unit** which comprises: **THE MODERNIZATION OF THE CURRENT ARCHITECTURE OF THE SAFE CITY SYSTEMS AND OF THE EXISTING GOVERNANCE RELATED TO THEIR USE THROUGH THE MANAGEMENT OF POLICIES REGARDING THE IMPLEMENTATION, MONITORING AND USE OF THESE SYSTEMS**.

II.4.3. Security of private and strategic objectives

The most important part of the civil security is the security of the private and strategic objectives. I will address the issue of the Airport Security, because I consider the airport the most complex type of objective currently available.

I had shown in the introduction that an airport has all the critical subcategories provided in Law 333/2003 and GO 301/2012, the Law on the protection of objectives, goods, values and protection of persons and its implementing Regulation. I also showed that all the public order security structures active in Romania operate in an airport, and in case of an incident are involved other international, national or local bodies and institutions.

II.4.3.1. Civil aviation security

Definition: *Civil aviation security is the combination of human and material measures and resources designed to protect the civil aviation against acts of unlawful interference that jeopardize the security of the civil aviation.* (EC Regulation 300/2008)

The air traffic is a vector of globalization. Globally, the airline industry is a major one involving about 1.6 billion passengers a year, 3.9 million employees, a turnover of $ 260 billion, 18,000 aircrafts, 15 million km airline network, 10,000 airports, 30 million tons of cargo annually.

The airports are, by definition, special objectives, economically and militarily strategic and, due to their complexity, are very difficult to protect. The aviation industry wants to attract passengers to the airlines, and it wants them to be accessible to those waiting for passengers. However, terrorists can use this to reach the control area in order to detonate bombs or shoot passengers.

II.4.3.2. Case study - Oradea International Airport

The development and economic potential of Oradea Municipality, as well as its geographical position make the Oradea International Airport an airport of European interest. Operating facilities and airport infrastructure are provided through customs, border, handling, as well as rescue and firefighting services, in accordance with CAT 6 OACI. At the same time, specific facilities are provided of which the passengers can benefit, such as cafes, spaces specially designed for *mother and child*, medical assistance, facilities for people with disabilities, travel and ticketing agencies, rent-a-car, etc.

Passenger safety: The emphasis is on the security and not on convenience.

Risk management in airport security is an element of the internal control system, with the help of which are discovered significant risks within the airport security system.

The development of a response strategy to risk factors consists in identifying each risk according to its type and degree of severity, and finding an appropriate response strategy for each case, details that make up the Crisis Management Plan of the airport. The crisis response strategies contain concrete actions regarding the responsibilities of each entity within the airport security system, the means of communication between the organizations, the change of the response method or the specifications that intervene on the established final results.

- PNR Directive (Register of Passengers' Names).
- Aircraft and runway safety.
- Perimeter detection subsystem.
- Access control subsystem.
- Surveillance subsystem with closed circuit television cameras.
- Classification of areas according to EC Regulation 300/2008.
- Passenger control and luggage control.
- Security regulations and working procedures
- International conventions and protocols. Community legislation.
- Airport security program
- Access to the air operations areas and security areas with restricted access.
- Known suppliers of airport and board supplies
- Communication scheme within the Crisis Center.

II.4.4. The opportunity to replace the human factor with automatic tactical security systems

The use of advanced technologies in the day-to-day operations of an enterprise is no longer surprising. However, the replacement of the human factor with technology remains a sensitive issue in the contemporary society.

We researched this issue in 2015-2016, and the research report was presented at the *IMT Oradea* International Conference on Scientific Communications in 2016, entitled *THE OPPORTUNITY OF REPLACING THE HUMAN FACTOR WITH TACTICAL AUTOMATED SECURITY SYSTEMS*. We will further develop the researched topic.

The purpose of this chapter is to study the security risk analysis in parallel with the economic opportunity, followed by a SWOT analysis and finally we will make an exercise in a case study on a concrete project implemented in the period 2015-2018 at the Water Company Arieș Turda SA (Compania de Apa Arieș Turda SA).

Following some specialized studies, it resulted that the margin of error of the burglary detection of the Automatic Tactical Security Systems is of maximum 5% (Ketcham, M., Ganokratanaaa, T., Srinhichaarnun, S., 2014).

We also conclude that the use of Automatic Tactical Security Systems is cheaper for 5 years of use than it is the Suman Security for one year.

Based on the research carried out in this chapter, it is easy to conclude that the partial replacement of the Human Factor with Automatic Tactical Security Systems is timely, efficient and financially profitable.

It is therefore recommended a comprehensive analysis, at a macro level of the security and

safety processes in the objectives and the attempt to streamline these processes from the points of view shown above.

II.4.5. Security, surveillance, monitoring systems and the video analysis of public domain

We have previously shown in Chapter II.4.4 the technical-economic opportunity of using the technical systems instead of the human factor. Also, in Chapter II.4.3 we analyzed a complete objective, namely, the international airport.

The purpose of this chapter is to study the interconnection and efficient use of all security equipments (burglary and fire alarm, access control, fences, smart barriers and parking, traffic lights, etc.), surveillance (public domain video surveillance, traffic, commercial area, industrial area, etc.), monitoring (pollution, air pressure, temperature, earthquakes, etc.) and analysis (traffic offenses, crimes, burglary, abandoned luggage, lost children, stray animals, etc.) a metropolis supplemented by the centralization of all these data, together with the data received from all other local UAT centers in the county in a centralized dispatch, county or regional, of the Inspectorate of Gendarmes.

II.4.5.1. The central dispatcher

Considering:

1. The fact that the face of a person represents personal data both according to the national legislation of Romania and according to the legislation of the European Union and the provisions of the GDPR.

2. Decision of the CURIA (Court of Justice of the European Union) ECLI:EU:C:2019: 1064: *Article 6 paragraph (1) letter (e) and Article 7 letter (f) of Directive 95/46/EC of the European Parliament of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, read in the light of Articles 7 and 8 of the Charter of the Fundamental Rights of the European Union, must be interpreted as not national provisions authorizing the establishment of a video surveillance system such as the system discussed in the main proceedings in the common parts of a residential building, in order to pursue legitimate interests in ensuring the protection and protection of persons and property without the consent of the data subjects, if the processing of the personal data carried out through the video surveillance system in question meets the conditions referred to in Article 7 letter (f), which is a matter of verification for the referring court* (CURIA, 2019).

We conclude that the Central Police Dispatch Office in the locality must be located in the local police station (communal, urban or municipal), with an active back-up to the County Inspectorate of Gendarmes (back-up both in terms of rendering and image analysis as well as in terms of image storage).

The location area of the dispatcher, both in the local police station and in the headquarters of the County Inspectorate of Gendarmes, will be in the administrative area, and the complete centralized data (information) will be classified by the Secret Service level. We will show further in this subchapter which individual categories of information will not have a classified character,

the persons who are going to operate them not being approved for the management of the classified information.

Within the County Inspectorate of Gendarmes, the Central Dispatch Office will be monitored non-stop by a dispatcher, agent or officer of the County Inspectorate of Gendarmes. The number of dispatchers per shift will be supplemented as needed or in case of specific actions.

The figures I recommend are a dispatcher for a maximum of 300 objectives and/or a maximum of 600 surveillance video cameras. If the total number of cameras in the Dispatcher will exceed 2500 cameras, I consider that the number of cameras per dispatcher can be increased to 1000 cameras, but only from the threshold of at least 3 active dispatchers per shift.

Considering the existing back-up at the County Inspectorate of Gendarmes, the communal and city Dispatchers do not necessarily have to be monitored non-stop, but only for specific actions or when direct registrations are desired, for efficiency.

When designing, installing and implementing the Dispatcher, all the security norms regarding the burglary, controlled access, PSI security and work safety norms, environmental protection norms, but also the protection norms against surges, short circuits or electric shocks will be taken into account. Under no circumstances will uncertified improvisations be accepted.

A. THE MECHANICAL-PHYSICAL SECURITY OF THE DISPATCHED OBJECTIVE

The objective will be arranged to accommodate a CENTRAL MONITORING DISPATCHER unit. When elaborating this documentation, the architectural divisions and the other installations related to the building (electrical, thermal, ventilation, etc.) are considered to have been made.

The integrated security system aims to secure the building in case of burglary or sabotage from the outside and inside of the building.

A.1. ELEMENTS REGARDING THE CONSTRUCTION

A.2. DESCRIPTION OF THE BURGLARY DETECTION INSTALLATION, TVCI SURVEILLANCE AND ACCESS CONTROL

B. TECHNICAL CAPACITIES FOR RECEPTION, STORAGE AND ARCHIVING, MONITORING AND ANALYSIS OF THE DATA/INFORMATION SUPPORTED BY THE CENTRAL DISPATCHER

In our study we will approach a complete dispatching system, characteristic of a *complete* local territorial administrative structure. More precisely, county seat municipalities, which have an international airport, and in the metropolitan area have both state border localities, border crossing points, exit to the highway, but also a resort of national and regional interest. Also, a regional administrative center: within its radius there is a Court of Appeal with all the affiliated structures, Regional Anti-Fraud Directorate, ISU Center, etc. Throughout all this territorial administrative apparatus with the related security and public order structures, we will try to implement in a complete Safe City System, which can be simplified according to the particularities of smaller UATs (cities, communes, etc.).

In a Complete Central Dispatch Office of a County Gendarme Inspectorate, must be monitored 3 main categories of systems:

1. Alarm systems:
    i. Burglar alarm systems
    ii. Fire alarm systems

2. Video Surveillance Systems
    i. Video Surveillance in Public institutions and of public interest
    ii. Public Domain Video Surveillance
    iii. Road and Pedestrian Traffic Video Surveillance
    iv. Video Surveillance in Institutions and in strategic and critical points
    v. Shopping Center Video Surveillance
    vi. Industrial Zone Video Surveillance
    vii. Video Surveillance in Public meeting areas (artistic and social events, sports matches, gyms, etc.)
    viii. Video surveillance in public transport

3. Auxiliary smart sensor networks
    i. Pollution quality monitoring (air, water, etc.)
    ii. Monitoring of the water pressure at hydrants and other critical points
    iii. Thermal monitoring for electrical and thermal + chemical installations for gas installations, district heating, etc.
    iv. Parking place monitoring
    v. Crowd monitoring (traffic, pedestrian areas, public events or shopping areas/centers, etc.)
    vi. GPS monitoring
    vii. Public transport monitoring
    viii. Weather sensor monitoring
    ix. Seismic sensor monitoring
    x. Etc.

At the level of the year 2020, there are specialized softwares that recognize the violations of road legislation and automatically print the contravention reports which also contain the photo proof of the legible registration number. The ascertaining agent only has to sign the deed after the verification and to sign the respective Minutes of contravention.

For category 3: The central dispatcher of the County Gendarme Inspectorate: we will study the design, installation and implementation of a centralized County Dispatcher, with a complete video analysis software that will have the possibility to access all the cameras of interest in the county.

It will function both as a back-up for storing and archiving the information, and as a main dispatcher for monitoring and alerting in case of an event.

B.2. As we showed at the beginning of this chapter, within the County Inspectorate of Gendarmes, the Central Dispatch Office will be monitored non-stop by a dispatcher, agent or officer of the County Inspectorate of Gendarmes. The number of dispatchers per shift will be supplemented as needed or in case of specific actions.

The figures I recommend are a dispatcher for a maximum of 300 technical alarm systems objectives and/or a maximum of 600 surveillance video cameras. If the total number of cameras in the Dispatcher will exceed 2500 cameras, I consider that the number of cameras per dispatcher can be increased up to 1000 cameras, but only from the minimum threshold of at least 3 active dispatchers per shift.

This Dispatcher will be equipped with ultra-high-performance video image analysis software with at least the following capabilities:

B.2.1. Objectives of public interest and Public Domain

- Recognition of Abandoned Objects
- Recognition of an Abandoned Child (recognizes a person with a height below e.g. 1.20m who is not accompanied for more than 2-5 minutes by the same adult/adults with whom he/she has previously been identified). It should also be mentioned that there are cameras that recognize based on the characteristics of the face the approximate age and sex of an individual.
- Recognition of Missing Objects (in case of vandalism, or incandescent street lamps)
- Recognition of a person who has fallen or is sick/nauseous
- Vehicle in an illegal place (sidewalk, park, etc.)
- Physical aggression
- Use of a weapon
- Accident on the public domain
- Burglary (broken wimdow, jumping over a fence)
- Smoke, fire and burning
- Object fallen *from the sky*
- Pedestrian on the tram line
- Facial recognition according to the database of wanted persons (identification of persons traced, e.g. generally traced (wanted) persons, Interpol database, etc. or even only suspects or persons of interest such as lost children, persons declared lost according to law or hooligans, known provocateurs, etc.).
- Recognition of masked people
- Number of persons with allocation by categories (children, cyclists, etc.)
- Recognition and alert to traffic congestion
- *Follower* recognition - (if a person is pursued to avoid small morals, physical aggression, rape, etc.)

We consider it very important that all communications are recorded for a period of at least 12 months. In this sense, all telephone lines will be connected to a voice recorder (e.g. Seka T-Rec 8) which will store and electronically archive all communications for a period of at least 12 months. The obligation to register calls is also provided in GD 301/2012, article 93 paragraph F, but only

for 30 days. Given the ultimate purpose of using these recordings, including in criminal investigations, and the importance of the Dispatchers and the conversations they have with them, I consider, however, that it is necessary to save the audio recordings for a period of at least 12 months.

B.2.2. Road Traffic

- LPR - recognition of registration numbers and saving in the database for at least 3 years of the following information: car registration number, photo of the registration number, date and exact time of the image capture, direction of travel
- Abnormal movement patterns and movements according to the pattern
- Road accident
- Fire detection, traffic fire
- Vehicles stopped in traffic
- Packages lost on the road, trees, fallen branches, stones, or other objects on the road that endanger traffic
- Counter vehicles by categories (motorcycles, motor vehicles, trucks, buses or road trains)
- Traffic congestion statistics
- Irregular parking
- Entering in prohibited areas
- Violation of the continuous line road marking
- Not respecting the red light at traffic lights
- Failure to comply with priority
- Failure to stop at a pedestrian crossing or at the railway barrier
- Walking Speed and *Speed Hero* Mode, i.e. recognized speedsters.
- Statistics on the places of repeated violation of the legal speed limit
- Statistics on average speed, average number of cars per day, per hour, at a certain time, etc.
- Illegal pedestrian crossings
- Illegal vehicles in traffic (expired numbers, carts, etc.)
- Low visibility (smoke, fog)

The video image analysis software will have the function of automatic recalibration of road traffic lanes in case the camera has been moved.

B.2.3. Video Surveillance in Institutions and in strategic and critical points
B.2.4. Video Surveillance in Centers, areas or shopping streets
B.2.5. Video Surveillance in Industrial Zones

B.2.6. Video Surveillance in Public meeting areas (artistic and social events, sports matches, gyms, etc.)

B.2.7. Video surveillance in public transportation
B.3. Auxiliary smart sensor networks

 i. *Pollution quality monitoring (air, water, etc.)*
 ii. *Monitoring water pressure at hydrants and other critical points*

  iii. *Thermal monitoring for electrical and thermal + chemical installations for gas installations, district heating, etc.*
  iv. *Parking monitoring*
  v. *Crowd monitoring (traffic, pedestrian areas, public events or shopping areas/centers, etc.)*
  vi. *GPS monitoring*
  vii. *Public transport monitoring*
  viii. *Weather sensor monitoring*
  ix. *Seismic sensor monitoring*
  x. *Other types of sensors and detection equipments*

II.4.5.2. Video Surveillance, Monitoring and Analysis System

II.4.5.3. Working procedures, priorities and a system of participation and sharing of resources

  Working procedures, priorities and a system of participation and sharing of resources for bodies and institutions directly or indirectly involved in the implementation, monitoring and use of the Safe City Systems are the second section of the theoretical part of the built-in unit: **THE MODERNIZATION OF THE CURRENT ARCHITECTURE OF THE SAFE CITY SYSTEMS AND OF THE EXISTING GOVERNANCE RELATED TO THEIR USE THROUGH THE MANAGEMENT OF POLICIES REGARDING THE IMPLEMENTATION, MONITORING AND USE OF THESE SYSTEMS.**

  In this chapter, we will study the possibility of developing and designing an interoperable framework system for the implementation and use of the Safe City systems, so that all th esecurity or defense structures can use this system, and at the same time there are no leaks of private or even classified information to persons who are not entitled to own them.

  II.4.5.3.1. Data transport

  II.4.5.3.2. Bodies and institutions directly involved. Participation in the Safe City System and access to their resources

  II.4.5.3.3. Bodies and institutions indirectly involved. Access to their resources

  II.4.5.3.4. Governance, priorities, execution and reporting of bodies and institutions involved in the monitoring and use of the Safe City System.

  II.4.5.4. Event scenarios and incident response simulation

  To test the proposed systems and their efficiency in case of an incident we will simulate tw major security incidents wich will engage both the Integrated Security Systems and the response of the human law enforcement involved.

  1. A terrorist attack consisting in the action of an individual hitting with a van the crowd of citizens from Unirii Square in Oradea with the purpose of causing a significant number of victims.

  Being a public square, it is impossible for such an event to be proactively prevented. In this case, we will simulate the terrorist attack and show how terrorists are identified, subsequently neutralized and detained by law enforcement.

  2. Attempt to board and aircraft of an COVID-19 infected person at Oradea International Airport.

  Having implemented a high-performance integrated security system (ISS) (the one designed in this thesis), this integrated security system ISS acts proactively so that it is impossible for the COVID infected person to bypass all automatic detection systems and the airport security

personnel. The person is stopped before passing the security zone. However, this citizen entering the "Departures" public area of Terminal 1 in the Oradea International Airport, will be in contact with hundreds of people in this area of the airport and will create an epidemiological risk incident.

We will show how the COVID infected citizen is detected, isolated and extracted by the security forces outside the airport. In addition to the police and ambulances, the SMURD service, the Gendarmerie, the Pubblic Health Department, etc. will intervene for restoring order and total disinfection of the terminal.

After restoring order, we will design a "traffic tunnel" through which passengers who have not had contact with the infected person and those who will board the aircraft in the next 24 hours will be routed and taken through Terminal 2 of Oradea International Airport, Terminal 1 remaining in quarantine 24h.

III. DEMONSTRATIVE EVIDENCE

The research that allowed this work is based on a solid empirical support, collected by respecting the methodological procedural rigors. The evidence collection methodologies used were both the direct observation and the participatory observation. The sources we used to collect the necessary evidence for the research were both academic papers (specialized studies, articles published in peer-reviewed journals) and technical projects of the Integrated Security Systems (SIS), technical data sheets of the equipment involved in SIS systems. At the same time, in order to have access to the opinions of some experts in the field, I also consulted interviews and debates published in specialized forums.

For data collection, we aimed to comply with the methodological rigors imposed by the priority principles, as they were theorized by Yin. In this regard, we operated with *a) multiple sources of evidence (two or more sources, which converge to the same findings), b) a database (it is the set of evidence gathered, not the final study report) and c) a logical sequence of evidence (explicit links between the data collected, the questions asked and the conclusions reached)* (Yin, 2005, p. 107). To ensure the level of objectivity required by the academic standards, these priority principles have been applied throughout the collection of the empirical data. Moreover, in the process of data collection we used an interdisciplinary range of methodologies from different sources, which is not strictly limited to the disciplinary boundaries of security studies, but also includes specialized works in the field of social sciences. The use of these interdisciplinary methodologies was necessary for two reasons: on the one hand, to place our research in the wider context of publications addressing security, and on the other hand, to minimize the chance of producing partial research, conclusions which are influenced by the databases used.

After becoming familiar with the interdisciplinary data collection procedures, the next step in building the research scaffolding was to create the project pattern. The pattern was built in compliance with the four established requirements: *the principle of construct validity, the principle of internal validity, the principle of external validity and fidelity*.

The four principles mentioned were applied for the collection of all eight types of sources operationalized during the investigations. The major sources used correspond to Robert Yin's taxonomy, shown in Table 4.1. (Yin, 2005, p.110) As Yin explains, there is no hierarchy of

sources, but rather an interdependence of them, as each source is complementary to the others, contributing to the overall unity of the research project.

In addition to the documentary information taken from the study of the academic and technical materials, this paper has as methodological originality the use of information taken directly by the author by visiting some security objectives of major interest. In this regard, the author visited the Canary Wharf Financial District in London, but also the NATO-HCOE military area, where he had the opportunity to directly observe the security systems used and their specific procedures, as recorded in the documentary bases of the mentioned objectives. The observations taken during these visits were made in accordance with the methodological requirements of the paper. In this sense, the data collection was formalized by recording own findings in standardized forms, field measurement of incidents of certain types of sensors in certain periods of time, but also of statistical results over a period of time from 1 to 5 years. At the same time, in addition to these quantifiable observations, we also recorded general observations regarding the overall architecture of the studied systems, procedures, objectives, regulations, legislation, and their directives.

These observations processed directly by the author were taken over during visits that were not intended exclusively for this purpose. In the context of these visits, the author took over other types of evidence, such as interviews with the agents involved, debates on the appropriateness and effectiveness of the technical or procedural improvements. The technique of direct observations was useful in taking over additional information about our topic, which is not already in the studies of other authors, thus contributing to the advancement of research in the field of security systems. At the same time, the direct observation led to a comparative assessment of the dimensions of the management of the architecture of the current Safe City systems and policies on the implementation, monitoring and use of these systems to ensure the decision-making power a true information base, both to maintain the state and security and public order, but also in critical moments or in the development of security and public order strategies.

Following the overall assessment of the evidence used and the methodologies used in their collection, it is necessary to explain in detail both the methodology of participatory observation and each type of evidence used.

The participatory observation is a methodology that differs from the observation practiced in everyday life by involving the observer in the management and supervision processes of the various projects that have been pursued. In this sense, the observer plays several roles in the observed projects, ranging from specialist consultant (risk assessor to physical security, interviewer and direct observer), to designer, technical engineer, and even to undertake functional activities specific to the installation of the technical security systems.

The types of data that were collected during the research are the following: internal documents of the Integrated Security Systems (SIS), specialized studies in the field of security studies, documents of some media materials relevant for the approached topic. From the category of internal documents of the Integrated Security Systems (SIS), were studied technical projects,

technical data sheets of the equipment, minutes of findings, reports of events and periodic statistics, and studies or formal evaluations of the objectives set by each system. From the category of specialized studies, we analyzed specialized articles from academic publications, both in the discipline of security studies and in related disciplines. From the category of media materials, we studied the media appearances on the security systems, but also websites relevant to the issue addressed.

In addition to the data already mentioned, we also used archives that systematize data on the architecture of the security systems. The analyzed archive data included registers, organizational documents, but also maps, statistics, graphs and organization charts. These archive materials contribute to the rigor of research, by ensuring its concordance with the existing research. Also, in the processing of archive data, we filtered the data relevant to our study, avoiding the use of redundant data, which would have hindered the dynamics of the research project and would have delayed its operationalization, but without providing substantial benefits.

A fundamental source of information for our research project was the interviews conducted as Director of the company Helion Security Srl. These interviews were conducted as part of the Helion Security's management and oversight responsibilities. The interviews were conducted on strategic objectives to ensure security at both national and regional levels. The results of these interviews have been processed in service documents, but these documents are placed, according to the legislation in force, in a confidential regime. As a result, the details of these interviews and the concrete data provided by them are not mentioned in this paper, but only the general observations taken from the interviewed subjects. The conduct of the interviews was aimed at achieving two objectives. First of all, the delimitation of an innovative own research direction, by flying over the problems faced by other agents specialized in the management of security systems. Secondly, the interviews aimed to obtain information that could be folded in the direction of research and that could not be obtained from other sources, available to the general public. In order to achieve these objectives, we asked the interviewed subjects open-ended questions, such as how, to allow the interlocutors to present their expertise on the topic approached in an autonomous way, not limited by the questions asked.

Another important source is represented by the websites of the international security organizations. These organizations periodically produce reports that systematize the latest discoveries in the field, being useful for connecting our research to all research in the field. In addition to the sites of these public actors, we also consulted the sites of some private actors, such as corporations that offer security systems, but also equipment manufacturers and installers of Integrated Security Systems (SIS).

To ensure the validity of the construct, but also the fidelity of the study evidence, we operationalized the data collected according to three principles: using multiple sources to collect evidence, building a database for the study and following a logical line of evidence. The first principle, the use of multiple sources of evidence, is a vital one to ensure the objectivity of the research and to avoid obtaining conclusions influenced by the data collected. Moreover, the use of evidence from different sources is fundamental for conducting a study that can be used to improve security systems. Given the recent events of a terrorist nature, which have made security a top priority, the need to produce research capable of improving the existing architecture is urgent.

Also, the use of multiple sources for evidence collection is fundamental to the chosen research methodology, namely the case study. The corroboration of multiple sources, from different related disciplines, is a specific aspect of case studies, which aim to produce interdisciplinary research, which analyzes an aspect from a plurality of perspectives, avoiding blocking in the conceptual plots of a single disciplinary field.

III.1. Demonstrative evidence for the primary unit: Modernization of the architecture of the Safe City systems, working procedures, priorities and a system of participation and sharing of resources for bodies and institutions directly or indirectly involved in the implementation, monitoring and use of this system

III.1.1. GD 301/2012 which completes and replaces GD 1010/2004 - Methodological norms for the application of Law no. 333/2003 on the protection of objectives, assets, values and protection of persons

III.1.2. ISO27001: 2013 certification standard that complements and replaces the ISO 27001: 2005 certification standard - Information Technology - Security techniques - Information security management systems - Requirements

III.1.3. M.A.I Instruction no. I9/2013 - regarding the performance of risk analyzes for the physical security of the units that are the object of Law no. 333/2003 on the protection of objectives, assets, values and protection of persons

III.1.4. Improving the A.I. (Artificial Intelligence) technology and the video analysis software, incident patterns (archive results and statistics)

III.1.5. Law no. 218/2002 regarding the organization and functioning of the Romanian Police

III.1.6. Law no. 550 of November 29th, 2004 on the organization and functioning of the Romanian Gendarmerie

III.1.7. Law no. 121/1996 on the organization and functioning of the Military Fire Brigade

III.1.8. Law no. 14/1992 on the organization and functioning of the Romanian Information Service, with the subsequent amendments and completions

III.1.9. Law no. 415/27.06.2002 for the organization and functioning of the Supreme Council of National Defense

III.1.10. Law no. 51/1991 on the National Security of Romania, with the subsequent amendments

III.1.11. National defense strategy for the period 2015-2019

III.1.12. Decision no. 271/2013 on the Cyber Security Strategy of Romania and the National Action Plan on the implementation of the National Cyber Security System

III.1.13. Law no. 215 of April 23rd, 2001 on the local public administration;

III.1.14. DECISION no. 585 of June 13th, 2002 for the approval of the National Standards for the protection of the classified information in Romania

III.1.15. DECISION no. 781 of July 25th, 2002 on the protection of the confidential information

III.1.16. Decision no. 1349/2002 on the collection, transport, distribution and protection, on the Romanian territory, of the classified correspondence

III.1.17. Schengen Directives and acquis

III.1.18. Law no. 535/2004 on preventing and combating terrorism - with the subsequent amendments

III.1.19. GD no.1077/2009 regarding the modification of GD no. 1869/2005 regarding PNAC-SECA (aeronautical security)

III.2. Demonstrative evidence for the contextual unit: THE NEED TO MODERNIZE THE ARCHITECTURE OF THE SAFE CITY SYSTEMS AND WORK PROCEDURES, PRIORITIES AND A SYSTEM OF PARTICIPATION AND SHARING OF THE RESOURCES FOR THE BODIES AND INSTITUTIONS DIRECTLY OR INDIRECTLY INVOLVED IN THE IMPLEMENTATION, MONITORING AND USE OF THIS SYSTEM.

III.2.1. Terrorist attacks in Europe since 2016.

III.2.2. GD 1010/2004 on the norms for the application of Law 333/2003 on the protection of objectives, assets, values and protection of persons proved to be obsolete after only 9 years and had to be updated with GD 301/2012, as detailed in point III.1.1.

III.2.3. Lack of long-term historical data.

III.2.4. Lack of regional coordination of both the security systems architecture and their use and action procedures

III.2.5. Lack of implementation of video analysis software with the help of A.I. (Artificial Intelligence) in the street surveillance systems installed so far.

III.2.6. Lack of intercommunication of the data collection sensors between the main Safe City systems (street surveillance, public domain surveillance, etc.) and the auxiliary systems (weather, pollution, seismic surveillance, etc.) installed so far.

III.2.7. Romania's entry into NATO and the EU represented some decisive moments in the modernization and development of Romania's national security. Virtually all security policies, both national and international, the national security strategy, the entire security context of Romania has undergone a complete transformation.

III.2.8. Data transport over insecure networks.

III.3. Demonstrative evidence for the bult-in unit: THE MODERNIZATION OF THE METHODS OF THE ARCHITECTURE OF THE CURRENT SAFE CITY SYSTEMS THROUGH THE MANAGEMENT OF THE POLICIES REGARDING THE IMPLEMENTATION, MONITORING AND USE OF THESE SYSTEMS IN A EUROPEAN CONTEXT

III.3.1. The integrated Safe City type Security Systems centralized at county level replace the classic Street Surveillance Systems with a registration server within the town halls.

III.3.2. Technological evolution of data collection through intelligent sensors

III.3.3. Analysis of data collected by A.I. (Artificial intelligence).

III.3.4. Long-term data archiving (alphanumeric information can be archived in databases with a history of up to 50 years, or even more)

III.3.5. Analysis of historical data (from archives and electronic databases) using A.I. (Artificial Intelligence) and creating incident patterns based on statistical analysis

III.3.6. Creating fiber optic infrastructures specially designed for Safe City systems or transforming classic internet connectivity networks into encrypted VPN networks.

III.3.7. Cross-border systems within the EU

III.3.8. Improvements and completions of organizational, procedural and governance nature of the decision of the policies regarding the implementation, monitoring and use of the Safe City systems

The data analysis showed that there is an imminent need for a policy transformation on Implementation (evaluation - financing - design - installation - quality verification), Monitoring (maintenance - surveillance - archiving) and Use (access - procedures - processes - decision governance - incident intervention) from a Reactive Policy to a Proactive Policy in order to ensure the decision-making power of a true information base, both for maintaining the security and the public order, but also in critical moments or in developing security strategies and public order.

It is easy to notice that in the last 20 years in Romania there has been only a Reactive policy for the implementation of the Safe City systems.

There were two main reasons for installing the systems:

1. Many events occurred at a critical point, and the UAT decided to install surveillance cameras at that point for a main coercive purpose.
2. There were non-reimbursable funds available, in which case the UAT or the institution decided to install Safe City Systems because *there was funding available*. We consider this policy fundamentally wrong because an effective concept is *to identify funding for known issues and not to quickly identify issues because we can spend some money.*

Of course, there are also cases where integrated systems have already been thought and designed at regional level, but these are isolated and represent an exception, not an implementation

rule. In this sense, we can see a pattern of these regional systems designed especially in regions with high levels of development (Bucharest, Cluj-Napoca, Timisoara, Oradea, etc.), in contrast to UTAs that have a lower level of development (unfortunately, majoritary), where even now are installed Independent Systems and without designing a subsequent interconnection of them.

We can easily see, for example, that in most counties of the country the County Police Inspectorate, the County Inspectorate of Gendarmes or the County Inspectorate of Emergency Situations do not have any access even to traffic monitoring systems of the communes of that county, much more to other objectives of major importance such as the County Hospitals, Sports Arenas, Water Dams and others.

IV. ANALYSIS OF THE DATA OBTAINED

Data analysis is part of the research strategy applied to the case study. It consists of examining, classifying, indexing and testing the evidence. In other words, data analysis involves their *quantitative and qualitative reorganization, in order to address the initial hypotheses of a study* (Yin, 2005, p. 135). Our case study was a challenge from the point of view of data analysis, because the strategies and techniques needed to perform the analysis could not be fully and directly taken from the bibliography. However, we have identified three strategies that build on plausible hypotheses a framework of plausible explanations, allowing certain case descriptions. By virtue of these strategies, *can be used five techniques specific to the analysis of the case studies: pattern matching, construction of explanations, analysis of time series, logical models and comparative synthesis* (Yin, 2005, p. 135).

For single case printing, the first four techniques are applicable. In our research we applied all the techniques mentioned above, but the challenge was the impulse to perform a quality analysis, which required increased attention to the empirical materials presented in detail in Chapter III, Demonstrative Evidence. To avoid the trap of a hasty interpretation, we have analyzed in detail the potential alternative interpretations.

Due to the lack of previous experience in operating with empirical data, the analysis of the evidence in the case study is necessarily limited. Due to the high complexity of research methods specific to data analysis, our analysis was limited to examining the evidence specified in the research hypothesis. In this regard, we analyzed the empirical materials that support the hypothesis that the management of the current architecture of the Safe City systems can be improved by adopting working procedures and by the superior management of human and material resources of the bodies and institutions involved in monitoring and using the system.

The empirical support brought to support the research hypothesis is a solid one, enough to prove the hypothesis regarding the management of the Safe City systems, but also to invalidate the alternative interpretations, contrary to our position. The analysis strategy operated with all the data, and the evidence was integrated into the taxonomy performed in the table below. The empirical material used was already in the form of graphs, tables and matrices, which eliminated the need to develop alternative models for classifying evidence during the actual analysis of the data. The technique used to integrate and explore alternative explanations is *pattern matching*.

V. CONCLUSIONS

Following our research we drew the following conclusions:

A Central Regional Dispatcher Office for Monitoring Data Sources (video cameras, smart sensors, etc.) can ensure that the decision-making power needs a database with real information, both to strengthen the state and security and public order, but also in critical moments or in case of the development of security and public order strategies.

The European authorities have become aware of this following the terrorist attacks of the last decade and have updated thje public policies, regulations and technical standards on security, public order and the model for the implementation and use of Integrated Safe City Security Systems. They also helped the national governments to jointly implement the guidelines, with Member States understanding the security risks and working together to combat the terrorism and to ensure the citizen security. The guidance guidelines complement a wider activity in trying to promote coherent and efficient approaches both by the institutions of force, but also by the central and local decision-making power, which urgently need these tools in the decision-making processes in order to manage effective security and public order policies. In particular, UTAs and the institutions indirectly involved in the implementation and monitoring of the Safe City systems must align their mode of action with the current needs.

The terrorist attacks of the last decade have also highlighted the importance of the information exchange between the EU Member States and led to the implementation of cross-border regional Safe City systems that are increasingly needed to increase the capacity of the EU states to manage risks.

Although it was considered sufficient, the reality of the authorities' support in the process of implementing the Safe City and Smart City Systems proved to be, in fact, superficial.

The implementation of a Central Regional Dispatcher Office for the monitoring of the Safe City Systems will institutionalize the interconnection and mutual complementarity between the local systems that already face major problems related to an efficient operability.

Removing the harmful effects caused by the independent implementation of the Safe City Systems at the level of each UTA, requires state intervention through appropriate regulations and policies to prevent the installation of public money of independent local systems that cannot be interconnected and does not communicate any kind of information to the main law enforcement forces or other critical beneficiaries in the county or region.

The progress made in the implementation from the operational perspective of Europol in collaboration with the state structures of security and public order, has determined the European Union to assume new attributions in the field of population monitoring.

The policies regarding the implementation and monitoring of the Safe City Systems in Romania are in a post-pioneering phase. There is an increasingly focused implementation of systems designed at the level of counties or regions, a modern method used for years in developed regions of the EU.

The Safe City systems are essential in predicting and limiting the hazards. The argument for limiting risks is based on analysis with modern A.I. (Artificial Intelligence) technologies of the historical statistical data currently existing at the level of 5-10 years and the notification of the Authorities in time on the risk of a future hazard. These notifications will be even more precise in the future, considering that we currently have a technology that can store and archive statistical data exactly for a period of up to 20 or even 50 years, these elements automatically developing a plus of accuracy in the incident analyzes carried out in the future.

Regarding the use policies, after analyzing the data we found that there is an imminent need for a transformation of the national policy on Implementation (evaluation - financing - design

- installation - quality verification), Monitoring (maintenance - surveillance - archiving) and Use (access - procedures - processes - governance of the decision - intervention in the incident) from a Reactive Policy to a Proactive Policy that will be able to ensure the decision-making power, the security system and the public order, but also the institutions indirectly involved a base of true information, both for keeping security and public order, but also in critical moments or in the development of security and public order strategies.

BIBLIOGRAPHY

A. Mulligan, C. E., & Olsson, M. (2013), *Architectural implications of smart city business models: an evolutionary perspective*, IEEE Communications Magazine, vol. 51(6), pg. 80–85.

ACCA, Accountacy Tuition Centre (1988) *Information Systems in Development and Operation*, Study Manual ATC, Ltd.

https://www.google.ro/search?q=ACCA,+Accountacy+Tuition+Centre+%281988%29+Informat ion+Systems+in+Development+and+Operation,+Study+Manual+ATC,+Ltd&ie=utf-8&oe=utf-8&gws_rd=cr&ei=RzYjV__eMcuNsgG4soeAAQ, (accesat la 30 aprilie 2016).

Adams, A. A., Ferryman, J. M. (2015), *The future of video analytics for surveillance and its ethical implications,* Security Journal, vol. 28, pg. 272–289.

Aguado, M., Jacob, E., Matias, J., Conde, C., Berbineau, M. (2009), *Deploying CCTV As an Ethernet Service Over the Wimax Mobile Network in the Public Transport Scenario,* 2009 IEEE International Conference on Communications Workshops.

Agustina, J. R., & Galdon Clavell, G. (2011), *The impact of CCTV on fundamental rights and crime prevention strategies: The case of the Catalan Control Commission of Video surveillance Devices,* Computer Law & Security Review, vol. 27(2), pg. 168–174.

Alexandrie, G. (2017), *Surveillance cameras and crime: A review of randomized and natural experiments,* Journal of Scandinavian Studies in Criminology and Crime Prevention, vol. 18, pg. 210–222.

Ali, F., Kwak, D., Khan, P., Islam, S. M. R., Kim, K. H., & Kwak, K. S. (2017*), Fuzzy ontology-based sentiment analysis of transportation and city feature reviews for safe traveling,* Transportation Research Part C: Emerging Technologies 2017 vol. C 77, pg. 33-48.

Ardestani, S. M., Jin, P. J., Feeley, C. (2016), *Signal Timing Detection Based on Spatial–Temporal Map Generated from CCTV Surveillance Video,* Transportation Research Record: Journal of the Transportation Research Board, vol. 2594, pg. 138–147.

Argyris, C. (1997) *Organizational Learning*, Addison Westey, Ed. Reading. https://www.google.ro/search?q=Argyris,+C.+%281997%29+Organizational+Learning,+A ddison+Westey,+Ed.+Reading.&ie=utf-8&oe=utf-8&gws_rd=cr&ei=0DIjV_XvNsSqsQGRvqSoAg, (accesat la 28 aprilie 2016).

Ashby, M. P. J. (2017), *The value of CCTV surveillance cameras as an invstigative tool: An empirical analysis,* European Journal on Criminal Policy and Research, vol. 23, pg. 441–459.

Beyon, D. (1990) *Information and Data Modeling*, Oxford Blakwell Sci.Publications. https://www.google.ro/search?q=Beyon,+D.+%281990%29+Information+and+Data+Mod eling,+Oxford+Blakwell+Sci.Publications.&ie=utf-8&oe=utf-8&gws_rd=cr&ei=By4jV8-lL4SwsAHSoZXoDA, (accesat la 30 aprilie 2016)

Birnhack, M., Perry-Hazan, L., German Ben-Hayun, S. (2017), *CCTV surveillance in primary schools: normalisation, resistance, and children's privacy consciousness,* Oxford Review of Education, vol. 44(2), pg. 204–220.

Bouma, H., Vogels, J., Aarts, O., Kruszynski, C., Wijn, R., Burghouts, G. (2013), *Behavioral profiling in CCTV cameras by combining multiple subtle suspicious observations of different surveillance operators,* Signal Processing, Sensor Fusion, and Target Recognition XXII.

Caplan, J. M., Kennedy, L. W., & Petrossian, G. (2011), *Police-monitored CCTV cameras in Newark, NJ: A quasi-experimental test of crime deterrence,* Journal of Experimental Criminology, vol. 7(3), pg. 255–274.

Caragliu Andreea, Nijkamp Peter (2009), *Smart cities in Europe, 3rd Central European Conference in Regional Science – CERS, 2009.* https://www.researchgate.net/publication/46433693_Smart_Cities_in_Europe, (accesat in 20 aprilie 2020).

Chen, M. (2012). *Towards smart city: M2M communications with software agent intelligence.* Multimedia Tools and Applications, vol. 67(1), pg. 167–178.

Chen Tao1, Xu Ling, Su Guofeng, Yuan Hongyong, Huang Quanyi (2014), *Architecture for Monitoring Urban Infrastructure and Analysis Method for a Smart-safe City*, Sixth International Conference on Measuring Technology and Mechatronics Automation, 2014.

Cheng, S.-T., Li, J.-P., Horng, G.-J., Wang, K.-C. (2013), *The Adaptive Road Routing Recommendation for Traffic Congestion Avoidance in Smart City,* Wireless Personal Communications, vol. 77(1), pg. 225–246.

Codrean, R. G. (2016), *"THE OPPORTUNITY OF REPLACING THE HUMAN FACTOR WITH TACTICAL AUTOMATED SECURITY SYSTEMS" (Oportunitatea inlocuirii factorului uman cu sisteme tactice automate de securitate),* IMT Oradea 2016 Conference, ANNALS OF THE UNIVERSITY OF ORADEA, Fascicle of Management and Technological Engineering, ISSUE #2, AUGUST 2016, http://www.imtuoradea.ro/auo.fmte/ https://imt.uoradea.ro/auo.fmte/files-2016-v2/Rares%20George%20Codrean%20-%20THE%20OPPORTUNITY%20OF%20REPLACING%20THE%20HUMAN%20FACTOR%20WITH%20TACTICAL%20AUTOMATED%20SECURITY%20SYSTEMS.pdf (accesat in 20 aprilie 2020).

Coeficienti criminalitate nationala 2012-2020, 2020, https://www.politiaromana.ro/files/pages_files/21-01-27-07-56-39Coeficienti_criminalitate_nationala_2012-2020.xlsx (accesat in 20 ianuarie 2021).

Costin, A. (2016), *Security of CCTV and Video Surveillance Systems,* Proceedings of the 6th International Workshop on Trustworthy Embedded Devices - TrustED '16.

Cognini, R., Corradini, F., Polini, A., & Re, B. (2014), *Modelling Process Intensive Scenarios for the Smart City,* Electronic Government, pg. 147–158.

Collin, S.M.H. (1990) *ISB Dictionary of Computing & Information* Technology, (Bilingual Specialist Dictionaries, Peter Collin Pub.,Ltd.Middlesex. https://www.google.ro/search?q=collin,+s.m.h.+%281990%29+dictionary+of+computing,+peter+collin+pub.&ie=utf-8&oe=utf-8&gws_rd=cr&ei=mjAjV9efEsOyswGKuqaoCg, (accesat la 30.aprilie 2016).

CURIA (2019), Hotararea CURIA (Curtea de Justiție a Uniunii Europene) ECLI:EU:C:2019:1064 http://curia.europa.eu/juris/document/document.jsf?text=&docid=221465&pageIndex=0&doclang=RO&mode=req&dir=&occ=first&part=1&cid=6895831 (accesat la 30 aprilie 2020).

Dadashi, N., Stedmon, A. W., Pridmore, T. P. (2013), *Semi-automated CCTV surveillance: The effects of system confidence, system accuracy and task complexity on operator vigilance, reliance and workload,* Applied Ergonomics, vol. 44(5), pg. 730–738.

Donald, F. M., Donald, C. H. M. (2014), *Task disengagement and implications for vigilance performance in CCTV surveillance,* Cognition, Technology & Work, vol. 17 (1), pg. 121–130.

Dumitrașcu, Eduard, Președinte ARSCM, (2018), *Ce este Smart City, Asociatia Romana pentru Smart City,* (Articol) tiparit in data de 31 martie 2018. https://romaniansmartcity.ro/ce-este-smart-city/, (accesat in 4 aprilie 2020).

Edelman, G., & Bijhold, J. (2010), *Tracking people and cars using 3D modeling and CCTV,* Forensic Science International, vol. 202(1-3), pg. 26–35.

Edmond, G. (2013), *Just truth? Carefully applying history, philosophy and sociology of science to the forensic use of CCTV images,* Studies in History and Philosophy of Science Part C: Studies in History and Philosophy of Biological and Biomedical Sciences, vol. 44(1), pg. 80–91

Ericsson (2020), *Ericsson achieves fastest 5G mmWave speed to date*, https://www.ericsson.com/en/news/2020/2/ericsson-achieves-record-5g-mmwave-speed (accesat la 30 aprilie 2020).

Galán-García, J. L., Aguilera-Venegas, G., Rodríguez-Cielos, P. (2014), *An accelerated-time simulation for traffic flow in a smart city,* Journal of Computational and Applied Mathematics, vol. 270, pg. 557–563.

Gerell, M. (2016), *Hot spot policing with actively monitored CCTV cameras: Does it reduce assaults in public places?*, International Criminal Justice Review, vol. 26, pg. 187–201.

Goold, Benjamin J. (2007), *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*, Oxford University Press, 224 pg, Oxford 2007.

Hempel, L., Töpfer, E. (2009), *The Surveillance Consensus,* European Journal of Criminology, vol. 6(2), pg. 157–177.

INSSE (2018), Institutul National de Statistica, *Rata infractionalitatii pe macroregiuni, regiuni de dezvoltare si judeţe: Selectati criteriile de interogare 1990-2015*, 2015 http://statistici.insse.ro/ (accesat in 10 iunie 2018).

Kerr, M., & van Schyndel, R. (2014), *Adapting Law Enforcement Frameworks to Address the Ethical Problems of CCTV Product Propagation,* IEEE Security & Privacy, vol. 12(4), pg. 14–21.

Ketcham, M., Ganokratanaa, T., Srinhichaarnun, S. (2014), *The intruder detection system for rapid transit using CCTV surveillance based on histogram shapes,* 2014 11th International Joint Conference on Computer Science and Software Engineering (JCSSE).

Kim, K., & Shin, D.-B. (2014), *The strategies on safe city making through hotspot analyses on crime,* KSCE Journal of Civil Engineering, 18(5), pg. 1511–1517.

Kitchin, R. (2013), *The real-time city? Big data and smart urbanism,* GeoJournal, vol. 79(1), pg. 1–14.

Klauser, F. (2009), *Interacting forms of expertise in security governance: the example of CCTV surveillance at Geneva International Airport,* The British Journal of Sociology, vol. 60(2), pg. 279–297.

Lawrence K. Gershwin (2015), *Global Trends Report*, *NIC 2000-02, December 2000.* Acest articol a fost aprobat pentru publicare de către National Foreign Intelligence Board sub autoritatea Directorului Central Intelligence Agency. Pregatit sub supravegherea National Intelligence Council, 2015.

Levi, S., Paldi, Y., Doron, M. B., & Silbinger, O. (2016), *Does one safe city model fit every community? evaluation of "Beterem in the City" in Israel.* Injury Prevention, 22 (Suppl 2), A117.1–A117.

Lin, K. J., Hou, T. K., Chiu, R. J. (2016), *Jitter-constrained camera scheduling in CCTV surveillance networks,* 2016 IEEE International Conference on Signal and Image Processing (ICSIP).

Lippert, R., Wilkinson, B. (2010), *Capturing crime, criminals and the public's imagination: Assembling Crime Stoppers and CCTV surveillance,* Crime, Media, Culture: An International Journal, vol. 6(2), pg. 131–152.

Liu, P., & Peng, Z. (2014), *China's Smart City Pilots: A Progress Report,* Computer, vol 47(10), pg. 72–81

Lucey, T. (1991) *Management Information Sistem*, DP publications Ltd. https://scholar.google.ro/scholar?q=Lucey,+T.+%281991%29+Management+Information+System,+DP+publications+Ltd.&hl=ro&as_sdt=0&as_vis=1&oi=scholart&sa=X&ved=0ahUKEwjC89T0y7PMAhXkO5oKHfPrBY0QgQMIHDAA, (accesat la 30 aprilie 2016).

Martinez-Balleste, A., Perez-martinez, P., Solanas, A. (2013), *The pursuit of citizens' privacy: a privacy-aware smart city is possible*, IEEE Communications Magazine, vol. 51(6), pg. 136–141.

Măgdoiu, L.D.,Rada, I.C. (2016) *The Antifragile of decisions adopted by Managers and Engineers Economist working in the Sector of Vulnerable Groups' Social Economy*, International Journal of Modern Communication Technologies & Research (IJMCTR), Engineering ResearchTM Publication, Volume 4, Issue-3. https://www.erpublication.org/admin/vol_issue2/upload%20Image/IJMCTR041301.pdf, (accesat la 28 aprilie 2016).

Möllers, N., Hälterlein, J. (2013), *Privacy issues in public discourse: the case of "smart" CCTV in Germany,* Innovation: The European Journal of Social Science Research, vol. 26(1-2), pg. 57–70.

Nerngchamnong, K., Kaviya, S., Fujii, Y., Yupapin, P. P. (2011), *World Heritage City Surveillance System by a Smart CCTV System,* Procedia Engineering, vol. 8, pg. 321–327.

Politia Romana, 2020, Anexa 19, *Model Proiect Sistem Tehnic de Alarmare,* https://www.politiaromana.ro/files/pages_files/16-10-20-01-55-18Anexa_19_Model_Proiect_STA.doc (accesat la 16 mai 2020).

Nasui, D., Oana, F. A., Sgarciu, V. (2010), *Wireless monitoring system in a safe city with Safe Mobile,* 2010 International Joint Conference on Computational Cybernetics and Technical Informatics.

Nițchi, Ș.I., Racovițan, D. et. al. (1996) *Bazele prelucrării informațiilor & Tehnologie informațională*, Deva, Ed. Intelcredo.

Parlamentul European (2015), *Colectarea datelor pasagerilor internaționali, 02-03-2015 - 12:33* https://www.europarl.europa.eu/news/ro/headlines/priorities/pnr/20150218STO24902/colectarea-datelor-pasagerilor-internationali , (accesat in 03.04.2020)

Parlamentul European (2016), *Parlamentul susține directiva privind registrul cu numele pasagerilor (PNR), Comunicat de presă SESIUNE 14-04-2016 - 12:38* https://www.europarl.europa.eu/news/ro/headlines/priorities/pnr/20160407IPR21775/parlamentul-sustine-directiva-privind-registrul-cu-numele-pasagerilor-pnr, (accesat in 03.04.2020)

Parlamentul European, De Bolle (2018), *Terorismul în UE: atacuri, decese, arestări - Securitate - Data actualizării: 05-09-2019 - 11:47, Creat: 25-07-2018 - 08:00, declaratie Catherine De Bolle,* https://www.europarl.europa.eu/news/ro/headlines/security/20180703STO07125/terorismul-in-ue-atacuri-decese-arestari, (accesat in 03.04.2020).

Parlamentul European, (2018), *Cum să oprim terorismul: măsurile UE (infografic), Securitate Data actualizării: 03-05-2019 - 12:58, Creat: 22-03-2018 - 14:32,* https://www.europarl.europa.eu/news/ro/headlines/security/20180316STO99922/cum-sa-oprim-terorismul-masurile-ue-infografic, (accesat in 03.04.2020).

Paroutis, S., Bennett, M., Heracleous, L. (2014), *A strategic view on smart city technology: The case of IBM Smarter Cities during a recession,* Technological Forecasting and Social Change, vol. 89, pg. 262–272.

Piza, E. L. (2018), *The crime prevention effect of CCTV in public places: A propensity score analysis,* Journal of Crime and Justice, vol. 41, pg. 14–30.

Piza, E. L., Caplan, J. M., Kennedy, L. W. (2013), *Analyzing the Influence of Micro-Level Factors on CCTV Camera Effect,* Journal of Quantitative Criminology, vol. 30(2), pg. 237–264.

Piza, E. L., Caplan, J. M., Kennedy, L. W. (2014), *Is the punishment more certain? An analysis of CCTV detections and enforcement,* Justice Quarterly, vol. 31, pg. 1015–1043.

Piza, E. L., Caplan, J. M., Kennedy, L. W., Gilchrist, A. M. (2015), *The effects of merging proactive CCTV monitoring with directed police patrol: A randomized control trial*, Journal of Experimental Criminology, vol. 11, pg. 43–69.

Piza, E. L., Caplan, J. M., Kennedy, L. W. (2017), *CCTV as a tool for early police intervention: Preliminary lessons from nine case studies*, Security Journal, vol. 30, p. 247–265.

Piza, E. L., Gilchrist, A. M., Caplan, J. M., Kennedy, L. W., O'Hara, B. A. (2016), *The financial implications of merging proactive CCTV monitoring and directed police patrol: A cost-benefit analysis,* Journal of Experimental Criminology, vol. 12, pg. 403–429.

Piza, E. L., Welsh, B. C., Farrington, D. P., Thomas, A. L. (2019), *CCTV surveillance for crime prevention,* Criminology & Public Policy, vol. 18(1), pg. 135–159.

Presidency.ro, Administratia Prezintentiala, (2015) *GHIDUL STRATEGIEI NAȚIONALE DE APĂRARE A ȚĂRII PENTRU PERIOADA 2015-2019*,

https://www.presidency.ro/files/userfiles/Ghid_SNApT_2015-2019_AP.pdf, (accesat in 03.04.2020).

Purshouse, J. (2014). *Beatrice von Silva-Tarouca Larsen, Setting the Watch: Privacy and the Ethics of CCTV Surveillance, Oxford: Hart Publishing, 2011, 226 pp*, The Modern Law Review, vol. 77(3), pg. 524–527.

Rada, I.C., Rada, Ioana C., Ursu, A.R., Kövendi, Z. (2014) *Management*, Oradea, Ed. Universității din Oradea.

Rada, I.C., Măgdoiu, L.D. (2016) *Forms of Communication and Strategies adopted by Managers and Economists Engineers in the "BLACK SWAN" Situation of Social Economy*, International Journal of Modern Communication Technologies & Research (IJMCTR), Engineering ResearchTM Publication, Volume 4, Issue-2. https://www.erpublication.org/admin/vol_issue2/upload%20Image/IJMCTR041205.pdf, (accesat la 28 aprilie 2016).

Reid, A. A., Andresen, M. A. (2012), *An evaluation of CCTV in a car park using police and insurance data,* Security Journal, vol. 27(1), pg. 55–79.

Richard George, Rob I. Mawby (2015), *Security at the 2012 London Olympics: Spectators, perceptions of London as a safe city*, Conferinta Security Journal (2015).

Rodríguez-Serrano, J. A., & Singh, S. (2012), *Trajectory clustering in CCTV traffic videos using probability product kernels with hidden Markov models,* Pattern Analysis and Applications, vol. 15(4), pg. 415–426.

Sarfraz, M. S., Shahzad, A., Elahi, M. A., Fraz, M., Zafar, I., Edirisinghe, E. A. (2011), *Real-time automatic license plate recognition for CCTV forensic applications,* Journal of Real-Time Image Processing, vol. 8(3), pg. 285–295.

Silva-Tarouca Larsen, B. (2011), *Setting the Watch Privacy and Ethics of CCTV Surveillance*, Hart Publishing Oxford, 2011.

Soori, U., Yuen, P. W. T., Ibrahim, I., Han, J., Tsitiridis, A., Hong, K., Richardson, M. (2011), *Colour invariant target recognition in multiple camera CCTV surveillance*. Optics and Photonics for Counterterrorism and Crime Fighting VII, Optical Materials in Defence Systems Technology VIII, Quantum-Physics-Based Information Security.

Suzuki, H., Fuwa, Y., Asano, D. K., Komatsu, M., Takeshita, Y., Futagawa, M., Kaneko, H. (2015), *Realization of a Safe and Secure Society using ICT in Shiojiri-City, Nagano Prefecture*, *Japan*, 2015 2nd International Conference on Information and Communication Technologies for Disaster Management (ICT-DM).

Taleb, N. N. (2010), *The Black Swan: The Impact of the Hghly Improbable (Lebăda neagră: impactul foarte puțin probabilului)*, București, Ed. Curtea Veche Publishing.

Taleb, N. N. (2014), *Antifragile: Things That Gain from Disorder (Antifragil: ce avem de câştigat de pe urma dezordinii)*, Bucureşti, Ed. Curtea Veche Publishing.

The Economist (2019), *Safe Cities Index 2019, Urban security and resilience in an interconnected world,* https://safecities.economist.com/wp-content/uploads/2019/08/Aug-5-ENG-NEC-Safe-Cities-2019-270x210-19-screen.pdf, (accesat in 4 aprilie 2020).

Trochim, W. (1989) *Outcome pattern matchingand program theory*, Evaluation and Program Planning, 12, pp.355-366.

Tsichritzis, D.C., Lochovsky, F.H., (1982), *Hierarchical data-base management: A survey.*, https://dl.acm.org/doi/10.1145/984382.984389 , (accesat in 4 aprilie 2020).

Ţigănoaia, B-D. (2013) *Asigurarea securităţii informaţiilor în organizaţii*, Iaşi, Ed. Institutului European.

Vachon, F., Vallières, B. R., Suss, J., Thériault, J.-D., Tremblay, S. (2016), *The CSSS Microworld*. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 60 (1), pg. 265–269.

Warnick, B. (2007), *Surveillance cameras in schools: An ethical analysis. Harvard Educational Review*, vol. 77, pg. 317–343.

Watters, C. (1992) *Dictionary of Information Sciences and Technology*, Academic Press. Inc. https://www.google.ro/search?q=Watters,+C.+%281992%29+Dictionary+of+Information+Sciences+and+Technology,+Academic+Press.+Inc.&ie=utf-8&oe=utf-8&gws_rd=cr&ei=QDgjV93ZGIyzsQGrpoyIAg, (accesat la 30 aprilie 2016).

Williams, D., Ahmed, J. (2009), *The relationship between antisocial stereotypes and public CCTV systems: exploring fear of crime in the modern surveillance society,* Psychology, Crime & Law, vol. 15(8), pg. 743–758.

Yin, R.K. (2005). Case Study Research. Design and Methods, Sage Publications, Thousand Oaks, London, New Delhi.

***** Centrul Naţional de Răspuns la Incidente de Securitate în Sistemele Informatice (CERT-RO), *Contramăsuri*, https://www.google.ro/search?q=Centrul+Na%C8%9Bional+de+R%C4%83spuns+la+Incidente+de+Securitate+%C3%AEn+Sistemele+Informatice+%28CERT-RO%29,+Contram%C4%83suri&ie=utf-8&oe=utf-8&gws_rd=cr&ei=CbooV5j8NoqqsAHWxI3IAw, (accesat la 3 mai 2016).

***** Centrul Naţional de Răspuns la Incidente de Securitate în Sistemele Informatice (CERT-RO), *Managementul riscurilor*, https://www.google.ro/search?q=Centrului+Na%C8%9Bional+de+R%C4%83spuns+la+Incidente+de+Securitate+%C3%AEn+Sistemele+Informatice+%28CERT-RO%29,+Managementul+riscurilor&ie=utf-8&oe=utf-8&gws_rd=cr&ei=IrcoV9uSIsSn6ATXnaKAAw, (accesat la 3 mai 2016).

***** Centrul Naţional de Răspuns la Incidente de Securitate în Sistemele Informatice (CERT-RO), *Incidente de securitate*, https://www.google.ro/search?q=Centrului+Na%C8%9Bional+de+R%C4%83spuns+la+Incidente+de+Securitate+%C3%AEn+Sistemele+Informatice+%28CERT-RO%29,+Incidente+de+securitate&ie=utf-8&oe=utf-8&gws_rd=cr&ei=HrgoV_HrJomosAHt546YAw, (accesat la 3 mai 2016).

***** Centrul Naţional de Răspuns la Incidente de Securitate în Sistemele Informatice (CERT-RO), *Vulnerabilităţi*, https://www.google.ro/search?q=Centrul+Na%C8%9Bional+de+R%C4%83spuns+la+Incidente+de+Securitate+%C3%AEn+Sistemele+Informatice+%28CERT-RO%29,+Vulnerabilit%C4%83%C8%9Bi&ie=utf-8&oe=utf-8&gws_rd=cr&ei=KrkoV8S4DsujsgGg2JygAQ, (accesat la 3 mai 2016).

***** Convenţia privind aviaţia civilă internaţională, semnată la *Chicago* la 7 decembrie 1944 la care România a aderat prin *Decretul nr. 194/1965 din 24/04/1965 privind aderarea Republicii Populare Române la Convenţia privind aviaţia civilă internaţională, semnată la Chicago la 7 decembrie 1944, cu unele amendamente aduse ulterior acestei convenţii - denumită în continuare "Convenţia de la Chicago"*;

SAFE CITY IN THE CONTEXT OF THE TERRORIST THREATS AND CRIME IN THE EUROPEAN UNION.

CASE STUDY: ORADEA MUNICIPALITY

***** Convenția referitoare la infracțiuni și la anumite alte acte săvârşite la bordul aeronavelor, încheiată la *Tokyo* la 14 septembrie 1963 la care România a aderat prin *Decretul nr. 627/1973 din 21/11/1973 privind aderarea Republicii Socialiste România la Convenția referitoare la infracțiuni şi la anumite alte acte săvârşite la bordul aeronavelor, încheiată la Tokyo la 14 septembrie 1963*;

***** Convenția pentru reprimarea capturării ilicite a aeronavelor, încheiată la *Haga* la 16 decembrie 1970 ratificată de România prin *Decretul nr. 143/1972 din 19/04/1972 privind ratificarea Convenției pentru reprimarea capturării ilicite a aeronavelor, încheiată la Haga la 16 decembrie 1970 – denumită în continuare "Convenția de la Haga".*

***** Protocolul pentru reprimarea capturării ilicite a aeronavelor, încheiat la Beijing pe 10 septembrie 2010 (este un protocol suplimentar al Convenției de la Haga).

***** Convenția pentru reprimarea actelor ilicite îndreptate contra securității aviației civile, încheiată la *Montreal* la 23 septembrie 1971 ratificată de România prin *Decretul nr. 66/1975 din 30/05/1975 privind ratificarea Convenției pentru reprimarea actelor ilicite îndreptate contra securității aviației civile, încheiată la Montreal la 23 septembrie 1971*;

***** Convenția cu privire la marcajul explozibililor plastici și în folie în scopul detectării, adoptată la *Montreal* la 1 martie 1991 la care România a aderat prin *Legea nr. 139/1998 din 29/06/1998 pentru aderarea României la Convenția cu privire la marcajul explozibililor plastici şi în folie în scopul detectării, adoptată la Montreal la 1 martie 1991 - denumită în continuare "Convenția de la Montreal".*

*****H.G. 196/2005 *privind aprobarea Strategiei Ministerului Administrației şi Internelor de realizare a ordinii și siguranței publice, pentru creşterea siguranței cetățeanului şi prevenirea criminalității stradale*, publicat în Monitorul Oficial, Partea I nr. 243 din 23 martie 2005.

***** Hotararea de Guvern 301/2012 *pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecția persoanelor,* Publicat în MONITORUL OFICIAL nr. 335 din 17 mai 2012 http://legislatie.just.ro/Public/DetaliiDocument/138059, (accesat la 03 aprilie 2020).

***** H.G. nr. 353/2002 *în legătură cu aprobarea normelor privind protecția informațiilor NATO în România*, publicată în Monitorul Oficial nr. 315 din 13 mai 2002, http://www.legex.ro/Hotararea-353-2002-31652.aspx , (accesat la 10 mai 2016).

***** H.G. nr. 585/2002 *privind standardele naționale de protecție a informațiilor clasificate*, http://www.orniss.ro/ro/585.html , (accesat la 10 mai 2016).

***** H.G. nr. 781/2002 *privind protecția informațiilor secrete de serviciu*, publicată în Monitorul Oficial Partea I nr. 575 din 5 august 2002. http://legislatie.resurse-pentru-democratie.org/legea/HG-781-2002.php, (accesat la 10 mai 2016).

***** Hotărârea nr. 779/2015 pentru aprobarea Strategiei naționale de ordine și siguranță publică 2015-2020. Publicat în Monitorul Oficial al României nr. 763 din 13 octombrie 2015. https://lege5.ro/Gratuit/haydeojtha/hotararea-nr-779-2015-pentru-aprobarea-strategiei-nationale-de-ordine-si-siguranta-publica-2015-2020 , (accesat la 03 aprilie 2020).

***** HOTĂRÂRE nr. 1.349 din 27 noiembrie 2002 privind colectarea, transportul, distribuirea și protecția, pe teritoriul României, a corespondentei clasificate, Publicat în MONITORUL OFICIAL nr. 909 din 13 decembrie 2002 http://legislatie.just.ro/Public/DetaliiDocumentAfis/40619, (accesat la 03 aprilie 2020).

***** LEGE nr. 14 din 24 februarie 1992 privind organizarea și funcționarea Serviciului Român de Informații, Publicat în MONITORUL OFICIAL nr. 33 din 3 martie 1992 http://legislatie.just.ro/Public/DetaliiDocument/2144, (accesat la 03 aprilie 2020).

***** LEGE Nr. 92 din 24 iulie 1996 privind organizarea și funcţionarea Serviciului de Telecomunicaţii Speciale, Publicat în MONITORUL OFICIAL NR. 169 din 30 iulie 1996 http://legislatie.just.ro/Public/DetaliiDocumentAfis/8502, (accesat la 03 aprilie 2020).

***** LEGE nr.121 din 16 octombrie 1996 privind organizarea și funcționarea Corpului Pompierilor Militari, publicat în Monitorul Oficial nr. 257 din 23 oct. 1996 http://www.cdep.ro/pls/legis/legis_pck.htp_act_text?idt=4019, (accesat la 03 aprilie 2020).

*****LEGE nr.191 din 19 octombrie 1998 privind organizarea și funcționarea Serviciului de Protecție și Pază, publicat în Monitorul Oficial nr. 402 din 22 oct. 1998 http://www.cdep.ro/pls/legis/legis_pck.htp_act_text?idt=18137, (accesat la 03 aprilie 2020).

*****LEGE nr.215 din 23 aprilie 2001 Legea administrației publice locale, publicat în Monitorul Oficial nr. 204 din 23 aprilie 2001 http://www.cdep.ro/pls/legis/legis_pck.htp_act_text?idt=27123, (accesat la 03 aprilie 2020).

***** LEGEA nr. 218 din 23 aprilie 2002 (*republicată*) privind organizarea și funcționarea Poliției Române, Publicat în MONITORUL OFICIAL nr. 170 din 2 martie 2020 http://legislatie.just.ro/Public/DetaliiDocument/157719, (accesat la 03 aprilie 2020).

***** Legea nr. 333/2003(**republicată**) *privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor* Publicat în MONITORUL OFICIAL nr. 189 din 18 martie 2014. http://legislatie.just.ro/Public/DetaliiDocument/45134, (accesat la 03 aprilie 2020).

***** Legea nr. 550/2004 *privind organizarea și funcționarea Jandarmeriei Române* publicată în Monitorul Oficial nr. 1175 din 13 decembrie 2004. http://legislatie.just.ro/Public/DetaliiDocument/57610, (accesat la 03 aprilie 2020).

***** Legea nr. 676/2002 *privind protecția datelor cu caracter personal în rețelele de comunicații*, publicată în Monitorul Oficial, Partea I nr. 1101 din 25/11/2004. http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-privind-prelucrarea-datelor-cu-caracter-personal-si-protectia-vietii-private-in-sectorul-comunicatiilor-electronice.html, (accesat la 10 mai 2016).

***** Legea nr. 677/2001 *pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date*, publicată în Monitorul Oficial nr. 790 din 12 decembrie 2001, http://legislatie.resurse-pentru-democratie.org/legea/677-2001.php, (accesat la 10 mai 2016).

***** Legea nr. 415/27.06.2002 de organizare și funcționare a Consiliului Suprem de Apărare a Țării.

***** Legea nr. 51/1991 privind Siguranţa Naţională a României, cu modificările ulterioare.

***** Legea nr.126/1995 privind regimul materialelor explozive – republicată în 2011.

***** Legea nr. 14/1992 de organizare și funcţionare a Serviciului Român de Informaţii, cu modificările și completările ulterioare.

***** O.U.G. nr. 105/2001 privind Frontiera de Stat a României, cu modificările și completările ulterioare.

***** H.G. 445 din 09.05.2002 pentru aprobarea Normelor metodologice de aplicare a O.U.G. 105/2001 privind frontiera de stat a României.

***** Directive și acquis Schengen.

***** Legea nr. 333/2003 privind paza obiectivelor, bunurilor si valorilor - cu modificările şi completările ulterioare.

***** Legea nr. 86/2006 privind Codul Vamal al României.

***** Legea 295/2004 privind regimul armelor de foc şi al muniţiilor- republicată.

***** Legea 535/2004 privind prevenirea şi combaterea terorismului - cu modificările ulterioare.

***** H.G. nr.1077/2009 privind modificarea H.G. nr.1869/2005 referitoare la PNAC-SECA.

***** Legea 149/2012 privind aprobarea Ordonanţei nr.17/2011 privind controlul calităţii în domeniul securităţii aviaţiei civile.

***** Legea protecţiei muncii nr. 319/2006, cu modificările şi completările ulterioare.

***** Normele metodologice de aplicare a Legii 319/2006.

***** HG 1146/2006 - Echipamente de muncă.

***** HG 1028/2006 - Utilizarea echipamentelor cu ecrane de vizualizare.

***** HG 1048/2006 - Echipamente individuale de protecţie.

***** HG 971/2006 - Semnalizările de securitate şi sănătate în muncă, cu modificările şi completările ulterioare.

***** ORDONANŢĂ DE URGENŢĂ nr. 30 din 25 aprilie 2007 privind organizarea şi funcţionarea Ministerului Afacerilor Interne, publicat in Monitorul Oficial nr. 309 din 9 mai 2007. https://www.mai.gov.ro/despre-noi/organizare/regulament-de-organizare-si-functionare/, (accesat la 03 aprilie 2020).

***** *Organizaţia Tratatului Atlanticului de Nord*, https://www.google.ro/search?q=Carta+Natiunilor+Unite&ie=utf-8&oe=utf-8&gws_rd=cr&ei=jXQoV43COYeVsgGmxaDoAw#q=Organiza%C8%9Bia+Tratatului+Atlanticului+de+Nord, (accesat la 3 mai 2016).

***** Regulamentul (UE) *nr. 468/2014 al BCE de instituire a cadrului de cooperare la nivelul Mecanismului Unic de Supraveghere între BCE, ANC şi AND*.

***** SR EN ISO 10001:2011 *Managementul calităţii. Satisfacţia clientului. Linii directoare pentru coduri de conduită în organizaţii*.

***** Parlamentul European, *Regulamentul UE nr. 1093/2010 de instituire a Autorităţii europene de supraveghere*.

***** SR EN ISO 31000:2010 *Managementul riscului. Principii şi linii directoare*.

***** SR EN ISO 9000:2015 *Sisteme de management al calităţii. Principii fundamentale şi vocabular*;

***** SR EN ISO 9001:2015 *Sisteme de management al calităţii. Cerinţe*.

***** SR EN ISO 9004:2010 *Conducerea unei organizaţii către un succes durabil. O abordare bazată pe managementul calităţii*.

***** SR EN ISO/CEI 27000:2013 *Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Privire de ansamblu şi vocabular*.

***** SR EN ISO/CEI 27001:2013 *Sistemul de Management al Securităţii Informaţiei*.

*****SR SR ISO 10004:2013 *Managementul calităţii. Satisfacţia clientului. Linii directoare pentru monitorizare şi măsurare*.

*****Strategia naţională de ordine publică 2010-2013 din 13 octombrie 2010 , Publicat în MONITORUL OFICIAL nr. 721 din 28 octombrie 2010. http://legislatie.just.ro/Public/DetaliiDocumentAfis/123096, (accesat la 03 aprilie 2020).

ACRONYMS

AI: Artificial Intelligence
ANAF: National Agency for Fiscal Administration
ARSCM: Romanian Association for Smart City
BNR: National Bank of Romania
CCTV: Closed Circuit Television
CURIA: Court of Justice of the European Union
DCJM: Central County Monitoring Dispatcher Office
DCM: Central Monitoring Dispatcher Office
DIRS: Integrated regional security dispatcher
DVR: Digital Video Recorder
ECAC: European Civil Aviation Conference
GDPR: General Data Protection Regulation
GPS: Global Positioning System
GD: Government Decision
IJJ: County Gendarme Inspectorate
IPJ: County Police Inspectorate
IJSU: County Inspectorate for Emergency Situations
ISU: Inspectorate for Emergency Situations
LPR: License Plate Recognition
MAI: Ministry of Internal Affairs
MApN: Ministry of National Defense
NATO: North Atlantic Treaty Organization
NVR: Network Video Recorder
OACI: International Civil Aviation Organization
OUG/GEO: Emergency Ordinance
PCA: Access Control Point
PCACS: Access control and security control points
PIR: Passive infrared sensor (Motion sensor with infrared technology)
PIU: Passenger Information Units
PNR: Passenger Name Record
PNSA: National Aeronautical Security Program
SIS: Integrated Security System
SRI: Romanian Information Service
SPP: Security and Protection Service
STS: Special Telecommunications Service
SUA/USA: United States of America
SWOT: strengths, weaknesses, opportunities, and threats (analysis of strengths, weaknesses, opportunities, threats)
TVCI: Closed Circuit Television
UAT: Territorial Administrative Unit
EU: European Union
VMS: Video Management System
VPN: Virtual Private Network

LIST OF FIGURES AND TABLES

Fig. III.2.4. Asymmetric key encryption (adaptation)
Fig. III.2.5. Public key encryption system (asymmetric)