Knowledge Driven Framework for realization of proactive criminalistics investigation in Combating Terrorism and Organized Crime in Montenegro with special focus on interception, collection and recording computer data

Prof. dr. Velimir Rakočević*
Faculty of law Podgorica
University of Montenegro

Prof. dr. Zoran Pavlović**
Assistant Professor criminal law and criminalistics
Faculty of Law for Commerce and Judiciary, University "Business Academy" Novi Sad,
Ombudsman of the Autonomous Province of Vojvodina, Republic of Serbia

Doc. dr Aleksandar R. Ivanović*****
Assistant Professor criminal law and criminalistics
International University of Novi Pazar.
Dean of Faculty of law sciences at International University of Novi Pazar,
Republic of Serbia

Abstract

The purpose of this work is to articulate a set of interlinked research propositions about knowledge management systems in relation to so-called proactive criminalistics investigations in the field of prevention and combating against serious sort of crime such as organized crime and terrorism. Moreover, this paper addresses missing links in literature between "know-what" and „know-how" in relationships between knowledge management systems and proactive criminalistics investigations, with special attention to use of information and technology to effectively create, apply, and communicate knowledge in organizations such as the criminalistics police of Republic of Montenegro. In this purpose authors point on organizational use and management of information and technology in proactive criminalistics investigations of organized crime and terrorism by finding that link between knowledge driven framework for fight against this sort of crime, and application of information and technology (specifically Digital Forensics knowledge), represents application of special investigative measure interception, collection and recording of computer data.

In relation with this, authors first describing nature of so-called proactive criminalistics investigation, by comparing it with reactive criminalistics investigation, also apostrophize the importance of implementation of proactive approach in police work by pointing out the benefits that they generate in the fight against severe sort of crime, and

* E-mail: *veljorakocevic@yahoo.com.*
** E-mail: *zoran.pav@hotmail.com.*
*** E-mail: *a.ivanovic@uninp.edu.rs.*

giving basic models and guidelines for it realizations in case of terrorism and organized crime. After that, authors emphasize the link between knowledge management and proactive criminal investigations, first by analyzing the type of knowledge on which proactive criminalistics investigation should be based on, and then associated use of modern information technology with the scope of effective realization of proactive criminalistics investigations in the case of organized crime and terrorism. As a key link between these two segments authors see application of special investigative measure interception, collection and recording of computer data. Because of that in the second part of the paper, authors analyzed provisions of application of this special investigative measure under the legislation of the Republic of Montenegro. At the end paper concludes with a discussion of various policy recommendations for future research.

This article is based on the application of current practical work of the police, judiciary and prosecution of the Republic of Montenegro through context positivist and deductive paradigm. Propositional methodology in this paper is used to hypothesize about the two interlinked domains of research interest – knowledge management and proactive criminalistics investigations of organized crime and terrorism. The task in this paper is to conceive of and begin to map out an initial set of research propositions that relate knowledge management systems to the proactive criminalistics investigations of organized crime and terrorism selected for their research potential within the larger domain of fight against these types of crime in general. Such a propositional methodology is an inductive–deductive exercise of hypothesis building based on distinct sources of empirical evidence drawn from the two key domains of interest for this paper which are examined below. The first domain is that of proactive criminalistics investigation, with a particular emphasis on knowledge conceptualized as intelligence knowledge as our focal research interest, and the second domain is knowledge management, with a specific focus on the digital forensic in use by police to gathering investigative (intelligence) knowledge in purpose to prevent materialization of criminal intent (committing of criminal offence) an obtaining evidence for punishment perpetrators for preparatory actions regard to criminal offence.

Keywords: *knowledge management, digital forensics, prevention, special investigative measures, interception, collection and recording of computer data, human rights.*

Introduction

In accordance with contemporary trends of crime, in which there is the distinction between proactive and reactive approaches, according to this we can distinguish the criminalistics investigation on proactive and reactive. Reactive criminalistics investigations are the classical approach to the study of crime, which is applied on the basis of knowledge about the manifestation of a particular criminal act, or on the basis of information on the committed criminal offense, in order to clarify it. In other words, they all represent a reaction to specifically manifested criminal event, or already undertaken actions of the committing of criminal offense (which can stay in attempt or be carried out to the end - executed criminal offence). On the other hand, proactive criminalistics investigations are applied in relation to criminal events which are likely to

be committed. And until reactive criminalistics activity is based on more or less visible knowledge such as consequences of criminal offence, traces and objects of the criminal offense, interviews of the victim of criminal offense, interviews of eyewitnesses and etc., organizing and realization of proactive criminalistics investigation is very difficult. Primarily, because it must be based on knowledge in relation to criminal intent and undertaken preparatory actions. The problem is because it is very difficult to come to the knowledge about criminal intent or preparatory actions, for example about terrorist attack or some offence from field of organized crime. Reason for difficulties in sense of gathering this knowledge is primarily due to high level of latency, conspiracy and secrecy of this activities, when terrorism and organized crimes are in question.

It should be noted that reactive criminalistics investigation were proved to be inadequate because the modern forms of crime such as organized crime or terrorism are characterized by far-reaching and mostly unavoidable consequences (death of a large number of people, destruction of property on a large scale, the input of large amounts of drugs on the market, the input of "dirty" money through "money laundering" into the legal economic flows in some country). On the other hand the perpetrators of these acts are mostly professional criminals, and committing of crime is well planned and organized, with use of contemporary information technologies. Because of all of these there is lack of evidence (material and personal) about their involvement in the crime, so reactive criminalistics investigation in many cases are unsuccessful, or have been dismissed due to lack of evidence. In relation with this what is mentioned above, in the late eighties and early nineties of the 20th century, due to the expansion of modern forms of crime that are characterized by a high degree of sophistication, organization, flexibility, mobility, misuse of modern technology and internationalization, pure reactive criminalistics reaction has proven to be insufficient in fight against contemporary forms of criminal manifestations. Because of that, in this period there was a discussion and the development of so-called pro-active criminalistics investigation. It should be noted that this does not mean that the police had not previously dealt with proactively work, but in this period for the first time in developed countries, in the late eighties and early nineties of the twentieth century began to appear new approaches in organization criminalistics activity, with the goal to be efficient on combating contemporary forms of criminal manifestations, such as problem-oriented policing, led-intelligence police work, criminalistics strategic approach and community policing etc. New approaches are basically had a redefinition of the police role in society, setting new strategic goals, organizational forms, and the introduction of new methods of operation with the intention to eliminate the weaknesses of the concept, which was dominant in the greatest period of the twentieth century (reactive or event-driven criminalistics approach). Although there are differences between various models of these relatively new approaches to the organization of criminalistics activity, but they have some common characteristics. First is reflected in a proactive role of police and second is knowledge-based management of police work.

In the Republic of Montenegro, as well as in whole region of Western Balkan, reactive approach in fight against crime, or reactive criminalistics investigations, still dominant in compared of proactive, or preventive approach. With this research we want to influence on the established practice in our country, as well as in whole of the Western Balkans region, in terms of countering serious forms of crime such as organized crime and terrorism, which is more reactive than proactive oriented, and

point on the way how knowledge management system linked with knowledge from the field of Digital Forensics can be used for the successful organization and implementation of proactive criminalistics investigations. In the next part of the paper we will point on the meaning and characteristics of proactive criminalistics investigation, and to describe knowledge driven framework for realization of proactive criminalistics investigation. It should be noted, that in this work we will briefly analyzing basic elements of these modern concepts of organization of criminalistics activities, and that we are not going to deal with operational issues like is, what is that what police or prosecutor's office leads to ground of suspicion that certain people are preparing some serious crimes because intrusion into these details will surpassed frameworks of this work. Instead that we will only focus on the knowledge driven framework for realization of proactive criminalistics investigations in combating of organized crime and terrorism, and within that a special issue we will give to knowledge management system and using of modern information technologies (Digital Forensics) through timely application of special investigative measure interception, collection and recording of computer data, as a core of proactive criminalistics investigations of this types of crime, with special emphasis on legal standards which prescribe the implementation of this measure in the Republic of Montenegro.

Contribution and Findings:

The aim is to take into consideration the features of contemporary forms of crime manifestation, as well as the fact that the implementation only classic reactive criminalistics investigation, and use of conventional operational-tactical and investigative measures and actions are often of limited scope, especially in countering of organized crime and terrorism. The authors emphasize the role and the importance of special investigative measure interception, collection and recording of computer data in fighting these forms of crime, with special emphasis on the criteria and conditions for their implementation according to the regulations of the criminal procedure legislation of the Republic of Montenegro. In this way authors are trying to point out that if the knowledge from the field of Digital Forensics applied in the context of proactive criminalistics investigations may have a preventive effect in terms of prevent a person to realize his criminal intent.

People from practice, so-called decision makers in police, security agencies, or prosecution office can on the base on the findings of this work improve its activity on the field of organization and realization proactive criminalistics investigation against organized crime and terrorism. Also, lawmakers can benefit from the results and make some necessary changes in the regulations of criminal procedural legislation of the Republic of Montenegro which refers to the implementation of special investigative measure interception, collection and recording of computer data, which can enhance activities in the field of fight against organized crime and terrorism. In addition, benefit from the findings of this paper may also have educational institutions that educate police personnel as well as future professionals from the field of Digital Forensics. Namely, the findings of this study can help them to improve curricula and thus increase the competences of students with investigative knowledge's.

Recommendations for Practitioners and Researchers:

Use of purely reactive criminalistics investigations in cases of serious crime, such as organized crime and terrorism is insufficient, and that there is a need for increasing application of so-called proactive criminalistics investigations. And in that actions timely implementation of knowledge from the field of Digital Forensic in form of special investigative measure interception, collection and recording of computer data have important role, because by its implementation we can prevent realization of criminal offence, with one side, and provide evidence for prosecution and condemnation of offenders because of preparation for execution of this type of crime.

Implementing of special investigative measure interception, collection and recording of computer data violate the rights and freedoms of citizens which are guaranteed by a huge number of international and national documents, but it is proved they are necessary and represent one of the most effective mechanisms of state in the fight against organized crime and terrorism. By this work authors want initiate the research and analysis of legal norms that regulate the use of these measures, as well as to explore the feasibility of this only in practice.

Impact on Society

This work should contribute to changing the approach in the fight against serious crime in Montenegro, such as organized crime and terrorism, in which instead of a reactive approach criminalistics, which is dominant in this area, focus should be shifted to the so-called proactive criminalistics approach, which must be knowledge driven and based on application of knowledge form the field of Digital Forensic. Thus, the authors expect that this work will contribute to improving the awareness and critical thinking among the police and prosecutor and sense of planning and implementation of proactive investigations of criminal activities.

1. The meaning and characteristics of proactive criminalistics investigations

Basis for taking proactive criminalistics investigations is suspicion that a particular person's (individually or in the group) engaged in illegal activities. In this regard, proactive criminalistics investigation may be manifested in two ways. The first focuses on a specific crime problem (for example, increased number of addicts' substance in a certain area, which indicates to the increased presence of the sale of narcotics). It is the so-called problem-oriented (proactive) criminalistics investigation. The second form is focused on certain persons or person as a possible carrier of criminal activities. It is a proactive criminalistics investigations aimed at targets. In both form the core of proactive criminalistics investigations makes police intelligence work, which is aimed at gathering knowledge about specific criminal risks and threats.

The essence of proactive criminalistics investigations include the pre-treatment, according to a criminal offense whose execution is expected, *i.e.* proactive steps are aimed at preventing criminal manifestations. Proactive criminalistics investigations were focused on any criminal event or a process that can lead to the commission of the crime, as well as to persons who are potential offenders. The goal of proactive

investigations is to identify potential criminal risks and threats and new forms of crime, in order to prevent the onset and reduce the potential damage, as opposed to reactive, whose goal is reflected in the discovery of the perpetrator and the preservation of evidence in order to initiate criminal proceedings for offenses that are already been made.

With respect to this goals, methodology of proactive criminalistics investigations is significantly different from the methodology and structure of reactive criminalistics investigations. Proactive criminalistics investigations usually start based on the collected intelligence to suggest that a particular individual or group planned to commit the crime, or to a particular area or object may occur commission of a crime. The proactive criminalistics activity in the fight against organized crime and protection of national security is, so to say, the "real" (timely) criminalistics protection from modern forms of crime. Conditionally, the "real" (timely) crime protection realized its function in vestibule of occurrence of adverse effects, *i.e.* before the start of materialization of criminal activity. In this regard, framework for proactive criminalistics activity should be based on certain knowledge, and that knowledge police capturing by giving answers to certain questions, which will then initiate further operational actions in sense of prevention of crime occurrence. Taking into account that this is an *ante delictum*, and not *post delictum* activities, "nine gold criminalistics issues" that are entering in the operational phase of *post delictum* criminalistics activity, here are useless because the criminal event has not yet occurred. So, to preventive criminalistics activity maintained its function must be set on so-called „golden questions" of preventive criminalistics whose answers need to be given in the stage of criminalistics control (Ivanović & Munižaba, 2013).

Table 1: The relationship between reactive and proactive criminal investigations

Description	Reactive criminalistics investigations	Proactive criminalistics investigations
Purpose	Detection, investigation and prosecution of crimes that are already committed.	Detection and prevention of the materialization of criminal intent.
Focus	Criminal offence which has happened in past.	A crime that might happen in the future.
Findings	Obtaining of evidence for judgment and punishment of perpetrator of committed criminal offence.	Discovering preparatory criminal actions and their prevention, obtaining evidence for preparatory criminal actions and also documenting the same in a purpose of prosecution, judgment and punishment its holders.
Framework	*"Nine gold criminalistics issues"* - What sort of crime was happened? - When criminal offence was happened? - Where is criminal offence happened? - How is criminal offence happened?	*„Golden questions" of preventive criminalistics* - Which circumstance, relationship, process or activity produced the idea of the realization of a criminal activity that is being prepared? - Which criminal activity has been preparing? - In what form and with what intensity will manifest?

Description	Reactive criminalistics investigations	Proactive criminalistics investigations
	- Why is criminal offence committed? - With what means criminal offence is committed? - With who is criminal offence committed? - Who is the victim of committed criminal offence? - Who is perpetrator of criminal offence?	- What are the possible modus operandi of offenders? - Which values are threatened and what consequences can be caused? - Who are the holders of the occurrence, or subjects of threat? - In which area criminal activity will manifest?

Answering on the above operational issues is carried out in a timely detection of phenomena that constitute criminal risks and threat to the security in the time of preparing a criminal offense and creates favorable conditions for the prevention of pre materialization, and thus prevent the endangerment and violation of the security situation. Thus, the function of crime proactive action, and action through the implementation of the criminalistics control to protect against modern forms of crime is reflected in the monitoring criminal environment and recognizing and detecting criminal risks and threats and preventing them before they come to the realization of criminal intent.

In connection with the above mentioned we can see that „golden questions" of preventive criminalistics determine and focusing criminalistics activity at the stage of the criminalistics control of crime on certain objectives. To perform its functions of the crime control must be based on the foundations of modern concepts of criminalistics activities, such as problem-oriented policing, intelligence-led police work, criminalistics strategic approach and community policing.

Specifically, the successful realization of proactive criminalistics activity is of great importance in a timely identification of the holders of future criminal activity with the aim prevent materialization of their intentions. A key part of the operational methodology of proactive police work is monitoring criminal milieu and application of methods of recognition phenomena in the environment, or the criminal milieu. The control of criminal and security risks and threats, and overseeing the criminal milieu through criminalistics measures, methods and tools requires a well-developed operational dimension of law enforcement agencies, in which criminalistics activity operating positioned so that its organization, implementation and interpretation of the operative material carried on manner that greatly increases the epistemological value of the material and thus increases the probability of success in the timely recognition, detection and control of criminal-security risks and threats in the stage of their formation, on the one side and gathering evidence of their existence on the other side. So, proactive criminalistics research must be scientifically based, *i.e.* be based on an analysis of data on the status and trends of criminal manifestations that threaten to the security of society. Based on these data, and using the scientific method, it is necessary to define the possible manifestations of criminal acts and security issues, as well as their development tendencies. Defining the possible criminal and security issues determines the focus of proactive criminalistics activity. After the determination of possible criminal and security issues, proactive criminalistics activity in the form of problem-oriented policing is directed toward neutralizing the conditions and causes which favor the occurrence of these problems (Goldstein, 1979).

Taking into account that the criminalistics activity in problem-oriented model of police work only focuses on criminal and security problem, which is not enough, there is a need for a parallel application of other forms of organization of criminalistics activity. In addition to the problem-oriented proactive criminalistics activities is necessary that the application of the concept intelligence-led police work. Specifically, a proactive criminalistics intelligence work is focused on the subjects or potential holders of criminal activity (Dvoršek, 2009). Therefore, it is very important to simultaneously focus criminalistics activity to the criminal and security problems, as well as potential subjects of threats. In addition to these ways of organizing criminalistics activity, for the effective realization of the criminalistics proactive protection is necessary and proactive strategic approach. Criminalistics strategic approach in order to protect society from modern forms of criminal manifestation is primarily reflected in the effective implementation of the objectives of criminal policy (Dvoršek, 2008). Thus, for example, if one of the goals of the criminal policy protection of economic system of counterfeit money, specifically counterfeit euros that criminal organizations inserted in financial flows, then using a strategic approach to shaping a proactive criminalistics strategy, which aims to identify and recognize the indicators that point to the possibility for the occurrence of this type of criminal manifestation of the territory of a country. From this defines criminalistics intelligence strategies derive the following requirements regarding the possible forgery of the euro in a given country: is there an intention of falsifying the euro in that country, whether domestic counterfeiters have the necessary knowledge to produce counterfeits, whether they have the necessary technical facilities and whether they have the necessary contact with other criminals for the establishment of a distribution network on the continent? Indicators by which they could respond to the set requirements are: finding counterfeit euros in the house owned by a famous forger, copying data printing euros and other technical information about making money by known counterfeiters on the territory of the country, try purchasing special copiers. If criminalistics intelligence activities receive a positive reply regarding the above intelligence requirements, then it is a sure sign that the potential danger of forgery euros in the territory of that country real and that it is necessary to develop an operational criminalistics strategy that aims to prevent this type of crime manifestation.

In this example we can see the necessity of coordination of problem-oriented and strategic approach to organized criminalistics activity with criminalistics intelligence activities. Also, for a proactive criminalistics activity is vital and selfless sharing of criminalistics intelligence knowledge between the various security agencies of the state. In fact, in practice, it is represented by a single rule that the security services of one country to a certain extent reserved to other security services of that state in respect of the exchange of criminalistics intelligence information. Thus, for example, after the terrorist attacks of September 11th showed that some security agencies of the United States had specific intelligence knowledge on the persons who are presumed to have committed terrorist attack, but that knowledge is not shared with other security agencies of the state. It is assumed that the situation is any chance was different, *i.e.* that the some of security services of the United States and shared information with other agencies, led to the conclusion mosaic of crime and timely adoption of the conclusion of the criminal intent of the person and the effective takeover measures to thwart the realization of these intentions.

Finally, it should be noted that in addition to the above, the effective implementation of proactive criminalistics activities is necessary practicing the concept of community

policing in order to establish a partnership between the citizens and the local community and members of the security services, especially the police. In this way, it also creates favorable conditions for the timely recognition criminal-security issues in the region, and criminal milieu, before there is a real threat to the values that protect by the national security system of a country.

Figure 1: Conceptual structure of proactive criminalistics investigation

2. Knowledge driven framework of proactive criminalistics investigation of organized crime and terorrism

As we look to the mentioned concepts of criminalistics activity which have proactive approach we can see that all of them are knowledge based. Because our work is focused on combating organized crime and terrorism through proactive criminalistics investigation which must be knowledge driven, in relation to this the following questions are imposed:

a) Which sort of knowledge is required for effective realization of this activity?

b) How we can gathering that knowledge?

c) What is it connection between obtaining of that knowledge and use of information technologies?

d) How knowledge management should be implemented in scope of proactive criminalistics investigation?

In order to reach the answers to these questions, first we must point out what it mean by knowledge and knowledge management. Knowledge present an important organizational resource. Organizations, in the modern day, are turning to knowledge

management initiatives and technologies to leverage their knowledge resources. Gottschakl (2007) seen knowledge-management as a systematic and organizationally specified process for acquiring, organizing, and communicating knowledge of employees i.e., knowledge workers, so that other employees may make use of it to be more effective and productive in their work. In the knowledge management literature is distinguished tree levels of knowledge: data, information and knowledge. According Awad and Ghaziri (2004) data is defined as unstructured facts, information is defined as structured data and attributes which can be communicated..., while knowledge is seen as information that has meaning ... and can be used to achieve some results. So, by this we can conclude that knowledge is a higher level of information and data. As Nissen (2002) argued that from the knowledge seekers point of view, data is put into context to create information, and actionable information, becomes knowledge (Järvenpää, Kopra & Lanz, 2016).

The American Productivity and Quality Center (APQC) defines knowledge management as an emerging set of strategies and approaches to create, safeguard, and put to use a wide range of knowledge assets, such as people and information. Thus, these assets flow to the right people at the right time so that they can be applied to create more value to the organization. Gupta e al. State that knowledge management is a process by which organizations are able to detect, select, organize, distribute and transmit vital information and experiences which would be used in activities like problem resolution, dynamic learning, strategic programming and decision making (Chang & Chung, 2014).

Criminalsitics activities of police in generally have two basic tasks: the generation of police knowledge (which refers primarily to the conclusions and giving answers on questions which relates to what crimes have been committed (repressive) or are likely to be committed (proactive – preventive – by whom, how and why...), and the production of evidence (which refers to the material that may be presented in the court to help establish that whether an alleged criminal offence has been committed or has been undertaken preparatory actions – organized crime and terrorism) (Fasihuddin, 2008). From that point of view knowledge management in police investigations is knowledge intensive and time critical and thus presents a substantial challenge to investigation managers. Successful investigation depends upon knowledge availability (Chen, Schroeder, Hauck, Ridgeway & Atabakhsh, Gupta, 2002). Police officers have to keep up to speed with the current legal and policy directions in relation to their work. Furthermore, they need to know the latest information on crime trends and potential threats to perform their duties effectively and efficiently (Luen & Al-Hawamdeh, 2001). We argue this presents a considerable challenge for knowledge sharing in a police service. Knowledge management is concerned with simplifying and improving the process of sharing, distributing, creating, capturing, and understanding knowledge. Hence, our argument is that knowledge is the most important resource in police investigations. Therefore, we can apply the knowledge-based perspective on organizations, which is derived from the resource-based theory of the firm to policing by stating that knowledge as a "strategic resource" is characterized by being valuable, scarce, non-imitable, nontransferable, non-substitutable, combinable, and exploitable (Dean, Fashing, Glomseth & Gottschalk, 2008).

Police investigation units represent a knowledge-intensive and time-critical environment. Successful police investigations are dependent on efficient and effective

knowledge sharing. Furthermore, Lahneman (2004) argues that successful knowledge management in law enforcement depends on developing an organizational culture that facilitates and rewards knowledge sharing. In this contest, detectives as knowledge workers are using their brains to make sense of information. Knowledge is often defined as information combined with interpretation, reflection and context. This combination takes place in the brains of detectives.

Gathering the knowledge that underpins a criminalistics investigation is a key task for an investigator. In fact, catching criminals cannot happen until an investigator first poses the knowledge provided by forensics, intelligence, and interviewing victims, witnesses, and interrogating suspects (Dean, Fashing, Glomseth & Gottschalk, 2008). Hence, this paper is a hypothesis building exercise into how to best gather the sort of investigative knowledge which is need for successful organization and realization of proactive criminalistics investigations of organized crime and terrorism, in the next part of the work we discus about this knowledge with correlation of implementing of modern information technologies. Namely, police work seems extremely knowledge intensive and from everything above we can see that it is actually intelligence knowledge, which main purpose is the identification of potential criminals *i.e.,* proactive intelligence or preventive intelligence or threat assessment. Gottschalk quotes Lahneman, that intelligence agencies were the world's first knowledge companies (Gottschalk, 2007).

In order to give answers to the above mentioned issues, and in purpose to fully point to the connection between knowledge management, application of modern information technologies and proactive criminal investigations of organized crime and terrorism, it is crucial to first say something about the knowledge management and activities of terrorist and organized criminal groups. The information and knowledge have long since become key resources of activities of terrorist and organized crime groups. They're in the criminal milieu and the illegal market tend to be more competitive and to strengthen its position by using information and knowledge. The activity of terrorist and organized criminal groups in illegal and legal market is enriched with information or knowledge by specialists from various fields which was hired by terrorist organization or organized criminal groups. They pay particular attention to interaction and exchange knowledge and information with groups from the environment, which enables them to plan and correct their strategies for work. On the other hand, they use rapid and constant technology changes, and development of information technology as a key resources of its development. Thus, terrorist groups and organized criminal groups become users of personnel which criminal activity converted into knowledge driven activity. In this way, their criminal activity takes on characteristics of a business strategy that is based on knowledge management. Accordingly, proactive criminalistics activity should be based on knowledge management in response to the strategic and knowledge driven action of terrorist and organized criminal groups.

Based on this we can conclude that it is a knowledge which has secret character, and which concerning with criminal intentions, plans, identity of group members who are preparing for criminal activity, undertaking preparatory work for the executed criminal activities and etc. Given that this is a knowledge which is based on information which are generally cannot be obtained from the so-called open sources (questioning of

suspects, hearing of witnesses, search of the apartment and seizure of documents, etc.) and on a public way, but only from classified or secret sources, and on way that no one else should know that police work on capturing of that information, we come to the implementation of knowledge from the field of Digital Forensics in proactive criminalistics investigation of organized crime and terrorism.

So in the next part of the work we will describe how knowledge from Digital Forensics can be used in crime prevention. Namely, due to investigation digital forensic is usually viewed as an mostly reactive approach that serves to discovering and obtaining of evidence for the crime which have been already committed, and that its preventive role mostly tantamount to general prevention or deterrent effect. This is corroborated by Srinivasan (2013) which in his work says that Digital Forensics is an important area of study for information security students because, while computer forensic investigation does not prevent the crime from occurring in the first place, it serves as a powerful deterrent for the criminals to know that their acts can be discovered and prosecuted. In connection with this, in the research we strive to point out that if the knowledge of Digital Forensics applied as part of proactive criminal investigations, it may have a very preventive effect in terms of special prevention, *i.e.* preventing a particular person to materialize their criminal intent.

3. Implementation of knowledge from field of digital forensics as the core of proactive criminalistics investigations

The fight against organized crime and terrorism requires a series of actions and measures intended to thwart the perpetrators of criminal acts to commit the criminal activity and avoid punishment. Although there are no generally considered definitions of these forms of crime, we can say with certainty that there is a consensus of most authors in terms of the constituent elements of these socially negative phenomena. Thus, by the majority, organized crime is defined as a permanent and organized criminal enterprise whose intention is to profit from illegal activities and its existence is held permanently by using force, threats, monopoly control, and/or by corrupting public officials. As for terrorism, we thought that the most acceptable definition is an official FBI one, according to which terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce governments, the civilian population, or any segment thereof, in furtherance of political or social objectives (Ivanović & Faladžić, 2011).

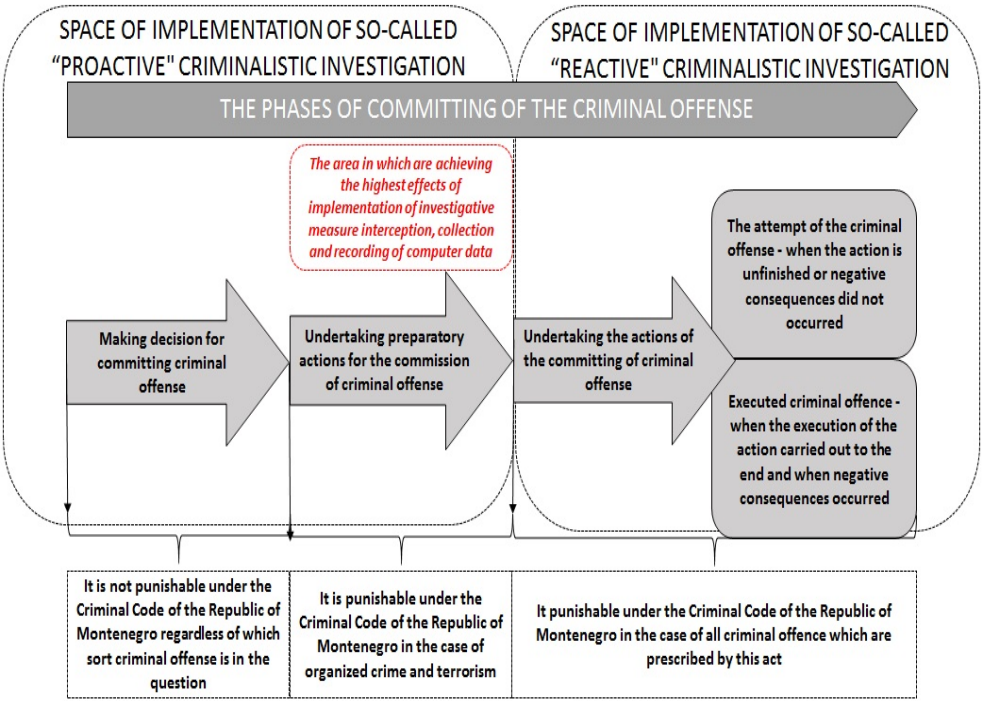
The main characteristics of these forms of criminal manifestation are: high level of organization, internationalization, recidivism, professionalization and specialization, the application of violence, cruelty and ruthlessness, and more frequent abuse of modern technical and technological achievements. For this reason, there is a need to find appropriate measures and resources in their suppression and prevention. The criminal legislation of many countries, the classical tools and methods applied in the prevention and suppression of the most difficult and most complex of modern criminal activities and organized crime, are replaced by new and more effective solutions, tools, methods and techniques. It is unthinkable to prevent and combat terrorism and organized crime without the application of modern tools, methods and techniques. Implementing these measures and actions violate the rights and freedoms of citizens which are guaranteed

by a huge number of international and national documents, but it is proved they are necessary and represent one of the most effective mechanisms of state in the fight against organized crime and terrorism. The introduction of specific procedures aimed at detecting and proving the acts of organized crime and terrorism in a more efficient way, which makes the arranging process to significantly deviate from the principles and traditional institutions of regular criminal proceedings. The focus of the proceedings is transferred to the earliest phase, instead of the investigation, evidence actions are taken in preliminary investigation which is understandable reason because the later would not be effective or are by their nature such that they afterwards can not be taken, for example., secret audio and visual surveillance of a suspect. Status of a suspect is obtained when there are grounds for suspicion that the person is preparing or participating in the preparation of criminal acts of organized crime. It is not required that a criminal offence should be committed, which means that the citizen becomes suspect earlier than in the normal procedure when the offense does not belong to organized crime.

For the effective implementation of these measures, in accordance with the European standards for the protection of human rights, the countries must, in addition to building the basic legal framework to enable implementation of measures and develop the appropriate by-laws and institutional structures and functional mechanisms, and with well-trained officers on the practical implementation of these measures.

The question is which is the best way for timely detection of undertaking preparatory actions and also documenting the same in a purpose of prosecution, judgment and punishment of perpetrators, and what is the common denominator for these activities. The answer to this question lies in the logistics work of criminal activity. Specifically, in order to jointly undertake preparatory criminal actions, there is need for communication between criminals or persons who are involved in criminal activity whose implementation is preparing, for example a terrorist attack. Criminals have long since become aware of the importance of secrecy at this stage of criminal activity, and because of this they avoids direct communication by phone. Instead communications by phone they usually prefer to communicate via encrypted e-mail, social networks such as Facebook, Skype, Viber, WatsApp etc. For example, in an attempt of the military coup that took place in July 2016 in Turkey, WathsApp was used as the main mode of communication by the put schists. In November terrorist group, which is suspected to be associated with a terrorist group Islamic State, has been arrested in Kosovo because of preparing terrorist attacks in the Balkans. In discovering and identifying these group were intercepting communications of its members through Skype. This form of communication through computer networks and systems is a common denominator for proactive actions, *i.e.* detection and prevention of criminal activities in the stage of preparatory actions and timely provision of evidence to punish them for the preparation of the crime. So that what some member of organized or terrorist group type through computer, mobile phones, smart phones, tablets or GPS devices can be intercepted, collected and stored and this fact makes it possible for the gathering of forensic computer evidence (Wolfe, 2001).

Figure 2: Review of the relationship between "proactive" and "reactive" criminalistics investigations and their connection with the phases of committing the criminal offense



As Irons and Ophoff (2016) arguing that access to computing and computing technology grows and as the use of computing resources and applications becomes even more widespread, the potential threat of cybercrime also grows. On the same way threat of application of computing resources on filed of organized crime and terrorism is also grows. So as Irons and Ophoff (2016) arguing there is also the need to put in place policy frameworks that will allow for digital investigations to be undertaken. As the initial hypothesis of our work is that proactive criminalistics investigations of organized crime and terrorism must be knowledge driven and based on application of information and technology (specifically Digital Forensics knowledge) and that the core of that activites represent application of special investigative measure interception, collection and recording of computer data, further in the paper we will focus on legal provisions for implementing this measure under criminal procedural law of Republic of Montenegro.

Therefore, the focus of proactive criminalistics investigations should be computer data which are generated by communication between persons who undertake preparatory activities for committing serious crime. Given that these are the data which are protected by right to the inviolability of privacy of correspondence, for their interception, collection and storage there is need for specific legal authorization. This is actually a special investigate measures which prescribing in national legislation is recommended by Convention on Cybercrime adopted in 2001st in Budapest.

4. The application of special investigative measures interception, collection and recording of computer data according to the legislation of the Republic of Montenegro

The application of special investigative measures interception, collection and recording of computer data is provided by articles 157, 158 and 159 of Criminal Procedure Code of the Republic of Montenegro. To this measure could be applied must be cumulatively met the following requirements. First, special investigative measure interception, collection and recording of computer data may be determined if there are grounds for suspicion exist that a person has individually or in complicity with others committed, is committing or is preparing to commit following criminal offences (article 158 CPC MNE):

1) for which a prison sentence of ten years or a more severe penalty may be imposed;

2) having elements of organized crime;

3) causing false bankruptcy, abuse of assessment, passive bribery, active bribery, trading in influence, abuse of an official position, as well as abuse of powers in economy, and fraud in the conduct of an official duty with prescribed imprisonment sentence of eight years or a more severe sentence;

4) abduction, extortion, blackmail, meditation in prostitution, displaying pornographic material, usury, tax and contributions evasion, smuggling, unlawful processing, disposal and storing of dangerous substances, attack on a person acting in an official capacity during performance on an official duty, obstruction of evidences, criminal association, disclosure of confidential information, breach of confidentiality of proceedings, money laundering, counterfeiting of money, forgery of documents, falsification of official documents, making, procuring or providing to others means and materials for forging, participation in foreign armed formations, arranging outcomes of competitions., unlawful keeping of weapons and explosions, illegal crossing of the state border and smuggling in human beings.

5) against the security of computer data (article 158 CPC MNE).

Second condition which must be cumulatively met is fact that evidence cannot be obtained in another manner or their obtaining would require a disproportional risk or endangering the lives of people (Article 157 CPC MNE).

So we can conclude that these measures can be applied against some person if we have grounds of suspicion that some of the offenses set forth in article 157 has committed, is committing or is preparing to commit by these person individually or in complicity with others. And that according to the circumstances of the case evidence cannot be obtained in another manner or their obtaining would require a disproportional risk or endangering the lives of people. This raises the question of the meaning of the term grounds for suspicion, given to that the Criminal Procedure Code of the Republic of Montenegro does not provide a definition of this term (Rakočević, 2014:256). In criminalistics science grounds for suspicion (indications, basic suspicions) are therefore the initial spark for start of criminalistics investigation, *i.e.* involvement of police officers on detecting and clarifying up of all relevant circumstances and facts that are related to a criminal activity. Grounds for suspicion are a form of probability based on the specific facts and circumstances which indicate the possible existence of crime or of some persons as a possible perpetrators. Grounds for suspicion are labeled low differential reach of, based on them to only a preliminary diagnosis in respect of

criminal acts or possible perpetrators. The literature also called sufficient suspicion or basic suspicions. The level of grounds suspicion exists when there are certain indications that indirectly indicate that some persons preparing to commit, are committing, or committed criminal offense. Seen from the point of truth, as much they could be true, at the same level they can also be false. Grounds for suspicion may occur before the crime was committed, during the committing the offense or after the commission of the crime. With respect to the elements of criminal offence grounds for suspicion may relate to: place, time, manner, motive of execution or identity of perpetrator.

So according to law, prosecutor could seek from the court (investigative judge) permission for the application of special investigative measure interception, collection and recording of computer data only if he could convince the investigative judge that there is ground for suspicion that the some person alone or with other persons preparing to commit, is committing or has already committed some of the criminal offenses set forth in article 157 of Criminal Procedural Code of Republic of Montenegro.

The second condition that must be fulfilled for the application of special investigative measure interception, collection and recording of computer data reflected in fact that evidence cannot be obtained in another manner or their obtaining would require a disproportional risk or endangering the lives of people. In the simplest way explained, such legal solution, mean that the implementation of this special investigative measure is not mandatory or primary, but it is optional and supplementary.

Which means that it will apply only if other conventional investigative measures could not achieve goals, or if their application would be risky. If we take in consideration that aim of proactive criminalistics investigation is discovering preparatory actions for the commission of criminal offenses, which criminals undertaking in strict secrecy, we can conclude that the classic measures such as monitoring, surveillance, collecting information will give almost no effect on the field of disclosing their criminal activities as well as providing evidence for the same criminal activities. In this regard, we believe that in most cases proactive criminalistics investigations of organized crime and terrorism there is a need for its implementation, which therefore means the fulfillment of the legal requirements for the application of special investigative measure interception, collection and recording of computer data.

Also measure interception, collection and recording of computer data may be also ordered against persons for whom there are grounds for suspicion that they have been conveying to the perpetrator or from the perpetrator of criminal offences referred to in Article 158 of the Criminal procedural code of Montenegro messages in connection to the criminal offence, or that the perpetrator has been using their telephone lines or other electronic communication devices (Article 175 paragraph 3 CPC MNE). In addition the law provides for the possibility that measure interception, collection and recording of computer data may be ordered against a person for whom an international arrest warrant was issued, or against a third party for whom there are grounds for suspicion that he is in direct contact with the person for whom there is an international arrest warrant (Article 175 paragraph 7 CPC MNE).

Measure interception, collection and recording of computer data shall be ordered via a written order by the investigative judge at the motion of the State Prosecutor containing a statement of reasons for implementation of this measure (Article 179 paragraph 1 CPC MNE). The Criminal procedure code provides an exception of the written procedure for determining the execution of this special investigative measure. So by way of exception, if the written order cannot be issued in time and risk of delay

exists, application of measure interception, collection and recording of computer data may begin on basis of a verbal order of the investigative judge. In that case, a written order must be obtained within 12 hours following the issue of the verbal order (Article 179 paragraph 1 CPC MNE). The motion and the order referred to the application of measure interception, collection and recording of computer data shall contain: data on the person against whom the measure is enforced, grounds for reasonable suspicion, the manner of measure enforcement, its goal, scope and duration (Article 179 paragraph 2 CPC MNE). The motion and the order for ordering measure interception, collection and recording of computer data shall become an integral part of the criminal file and should contain available data on the person against which is ordered, the criminal offence because of which is ordered, facts on basis of which the need to undertake it originates, duration deadline that needs to be suitable to achieving the objective of measure, manner, scope and place for the measure to be implemented (Article 179 paragraph 3 CPC MNE).

Based on the order of the investigating judge, the measure interception, collection and recording of computer data may last up to four months. For justified reasons, this measure may be extended against the same person and for the same criminal offence no longer than 18 months from the adoption of the first order for imposing secret surveillance measures (Article 179 paragraph 5 CPC MNE). It should be noted that such legal solution represents a significant prolongation of the measures bearing in mind that according to the previous law, the duration of secret surveillance measures were provided to a maximum of seven months. Enforcement of the measure shall be terminated by an order when the reasons for its application cease. Measure which enforcement was interrupted may continue for justified reasons against the same person and for the same criminal offence, based on an order. The maximum duration of the measure also includes the time during which the measure was interrupted. After the expiry of the periods referred to in this paragraph, enforcement of a measure may not continue and new measure may not be ordered for the same criminal offence and against the same perpetrator (Article 179 paragraph 5 CPC MNE).

In addition to the order for the application of measure of interception, collection and recording of computer data, the investigative judge shall issue a separate order containing solely the telephone number or e-mail address or the International Mobile Subscriber Identity (IMSI number), International Mobile Station Equipment Identity (IMEI number) and the internet protocol address (IP address) and the duration of the measure in question, and this order shall be delivered to enterprises (Postal agencies, other enterprises and legal entities registered for transmission of information) during the course of the application of the measure by the authorized police officers (Article 179 paragraph 8). Postal agencies, other enterprises and legal entities registered for transmission of information shall enable the authorized police officers to enforce the measure interception, collection and recording of computer data. Persons acting in an official capacity and responsible persons involved in the process of passing the order and enforcement of this measure shall keep as secret all the data they have learned in the course of this procedure (Article 179 paragraph 9).

If, during the enforcement of measures of interception, collection and recording of computer data, registered data and notifications which are referring to some other persons for whom grounds for suspicion exist that s/he had committed the criminal offence for which a measure of secret surveillance was ordered, or some other criminal offence, that part of the material shall be copied and forwarded to the State Prosecutor,

and it may be used as evidence only for criminal offences referred to in Article 158 of the Criminal Procedural Code of Republic of Montenegro (Article 179 paragraph 10 CPC MNE).

The special investigative measures interception, collection and recording of computer data shall be enforced by the authorized police officers in such a manner that the privacy of persons not subject to these measures be disturbed to the least extent possible (Article 160 paragraph 1 CPC MNE). Authorized police officer enforcing the measure shall keep records on each measure undertaken and report periodically to the State Prosecutor, that is, investigative judge on the enforcement of measures. If the State Prosecutor, *i.e.,* investigative judge ascertains that the need for enforcement of the ordered measure does not exist anymore, s/he shall issue and order on its discontinuation (Article 160 paragraph 5 CPC MNE). Upon the enforcement of measure the authorized police officers shall submit to the State Prosecutor a final report and other material obtained by the enforcement of measure (Article 160 paragraph 6 CPC MNE).

Should the State Prosecutor decide not to initiate a criminal procedure or if the data and information collected via this special investigative measure are not necessary for the criminal proceedings, s/he shall forward to the investigative judge the material obtained through the application of measure of interception, collection and recording of computer data, in a closed cover bearing the designation MSS, and the investigative judge shall order that the material be destroyed in the presence of the State Prosecutor and the investigative judge. The investigative judge shall compose a record thereon (Article 160 paragraph 7 CPC MNE). The investigative judge shall proceed in the same manner if the State Prosecutor orders that investigation be conducted against the suspect who was subjected to measure of interception, collection and recording of computer data, when the results obtained or parts of the results are not indispensable for the conduct of the criminal proceedings or when the person for whom there is an international arrest warrant is found (Article 160 paragraph 8 CPC MNE).

In cases where there is no need for further use in criminal procedure of registered data and notifications collected by this special investigative measure as is referred to in paras. 7 and 8 of article 160 of CPC MNE, data shall be considered as classified within the meaning of regulation prescribing data secrecy (Article 160 paragraph 9 CPC MNE).

If the special investigative measure interception, collection and recording of computer data was undertaken in contravention to the provisions of the present Code or in contravention to the order of the investigative judge or the State Prosecutor, the judgment may not be founded on the collected information (Article 161 paragraph 1 CPC MNE).

By prescribing of these procedures legislator has reduced the space for misuse of the special investigative measure interception, collection and recording of computer data in practice and also provide higher degree of protection of privacy and inviolability of communications and personal data in the case of implementation of this special investigative measure.

Before the material obtained through the enforcement of measure interception, collection and recording of computer data is destroyed, the investigative judge shall inform the person against whom the measure was undertaken, and that person shall have the right to examine the collected material (Article 162 paragraph 1 CPC MNE). By prescribing the obligation to inform the person against whom the measure was undertaken in a case where there is no further investigation or indictment against that

person, is also provided greater protection from possible abuse of this special investigation measure. If there is a reasonable concern that rendering information to the person against whom the measure was applied or examination of the collected material by such person could constitute a serious threat to the lives and health of people or could engender any investigation underway or if there are any other justifiable reasons, the investigative judge may, based on an opinion of the State Prosecutor, decide that the person against whom the measure was undertaken not be informed and allowed to examine the collected material (Article 162 paragraph 2 CPC MNE).

The State Prosecutor and the investigative judge shall, in an appropriate way (by coping records or official annotations without personal data, removal of an official annotation from the files and alike), prevent unauthorized persons, the suspects or their defense attorney to establish the identity of persons who have enforced the measure interception, collection and recording of computer data. If such persons are to be heard as witnesses, the court shall apply measures of protection of witnesses from intimidation which are prescribed in article 120-123 of Criminal Procedural Code of Republic of Montenegro (Article 159 paragraph 11 CPC MNE).

Prescribing possibility that from the report, which is made as a result of using special investigative measures, could be erased the names of the persons who have enforced the measure interception, collection and recording of computer data, very important in the sense of protection of their security. Moreover, we think that this should be defined in Criminal Procedural Code as an obligation, not an option. In fact, in practice, there are several cases where the persons who have enforced the measure interception, collection and recording of computer data, later were targeted and intimidated from some organized criminal groups. We are therefore of the opinion that the legislator should change this article in the sense that in the written reports of enforcing of this measure persons who have enforced this operation should be named under the code. And if there is a need to be heard as witnesses in the proceedings, then its identity could be discovered and court shall apply measures of protection of witnesses from intimidation. This solution we propose, because we believe that the identity of the person who have enforced this measure is not relevant for the suspect and his defense attorney, and because in practice there are almost no cases where there was a need to examine the person who conducted investigative measure such is interception, collection and recording of computer data.

Interception of communications is foreseen in the provisions of Article 180 of the Law on Electronic Communications of Republic of Montenegro. By provisions of this article the operator shall at his own expense provide the necessary technical and organizational conditions that enable interception of communications, which is in accordance with the provisions in Article 159 paragraph 9 of Criminal Procedural Code of Republic of Montenegro, according to which postal agencies, other enterprises and legal entities registered for transmission of information shall enable the authorized police officers to enforce the measure interception, collection and recording of computer data. In this article is prescribed that persons acting in an official capacity and responsible persons involved in the process of passing the order and enforcement of this measure shall keep as secret all the data they have learned in the course of this procedure (Article 159 paragraph 9 CPC MNE). Also in the Law on Electronic Communications is stressed the confidentiality of information relating to the content of the communication, the user data, traffic data and location-related communications and unsuccessfully established communication. It is forbidden to listen, eavesdrop or storing

the data content of the communication, or an interception or control by others, without the consent of that communication (Article 172 paragraph 2 LEC MNE). On the other hand, it is allowed technical storage or access to content or data communication without the consent of user of that communication, if the only purpose is to transfer the data over a public electronic communications network or, if necessary, on request of the user to operator provide this service (Article 172 paragraph 3 LEC MNE). Article 172, paragraph 4, prescribes the exceptionally possibility of listening, tapping or storage of content and information about communications, or an interception or control by others, without the consent of the user of that communication, only if this actions are necessary, appropriate and proportional to the measures for protection of national security, defense as well as to prevent the execution of the crime, investigation, detection and prosecution of criminal offenses and unauthorized use of systems for electronic communication, as well as in cases of providing assistance in search and rescue of people and when it is necessary to protect the lives and health of people and property, in accordance with the law. Further, the operator is obliged to provide facilities for the interception of communication in accordance with the conditions laid down in Article 172, paragraph 4, by order of the competent state bodies in accordance with the law. (Article 180 paragraph 2 LEC MNE). The operator shall, together with the relevant state authorities on whose request doing the legal interception of communications, provide a permanent record about this measure and that data which are collected under legal interception of communications shall be kept as an official secret (Article 180 paragraph 3 LEC MNE). Necessary technical and organizational requirements for the interception of communications under Article 180 of the Law on Electronic Communications of Republic of Montenegro prescribed by the Ministry for Information Society and Telecommunications, in agreement with public authorities responsible for internal affairs and security (Article 180 paragraph 4 LEC MNE). Operator which performs technical and program upgrades in its network or implementing new electronic communications services which have an impact on the lawful interception of communications, is obliged to inform about the upgrade or the implementation the competent authorities for the interception of communication at least six months before upgrading its networks or deploy new services (Article 180 paragraph 5 LEC MNE).

This law prescribes the duty of the operator to retain certain traffic data and location data, as well as relevant information necessary for the identification and registration of subscribers – legal entities and individuals, to the extent that these data are generated or processed, for the needs of defense and national security, and to prevent the execution of the crime, investigation, detection and prosecution of perpetrators of criminal acts and to provide assistance in search and rescue of people, protection of life and health of people and property, in accordance with the law (Article 180 paragraph 1 LEC MNE). The obligation to retain data applies to data on unsuccessful calls, the data are generated and processed with the telephone service provider or registered with the Internet service from operators (Article 180 paragraph 2 LEC MNE). The obligation to retain data does not apply to data that reveal the content of electronic communications (Article 180 paragraph 3 LEC MNE). The operator shall provide in its network the necessary technical and organizational conditions that allow authorized state authorities to download the retained traffic data and location data, as well as relevant data necessary for the identification and registration of subscribers. The retention period is limited in the range of six months to two years from the date of performing communication (Article 180 paragraph 4 i 5 LEC MNE).

As regards the categories of data which should keep there are the information necessary to monitor and determination the origin and destination of communication, determination the location of the participants of communications, determination the date, time and duration of a communication, determining the type of communication, the type if communications equipment of user or equipment used for the purpose of communication and determine the location in the case of mobile communication equipment (Article 182 paragraph 1 LEC MNE). In relation to security of retained data operator is obliged to ensure that the retained data be with the same quality and the same degree of safety and protection as well as the corresponding data on the network. It is also required to ensure with appropriate technical and organizational measures that retained data are protected from the illicit or accidental destruction, loss or alteration, unauthorized or unlawful storage, processing, access or disclosure. Retained data can be accessed only by persons authorized by the operator. Operators duty is that retained data, with the exception of data which is accessed and stored, destroy at the end of the specified retention period. Control over the implementation of these measures doing the authority responsible for the protection of personal data. (Article 183 LEC MNE).

In addition to the Code of Criminal Procedure and the Law on Electronic Communications interception of electronic communication is provided for by the Law on the Agency for National Security (ANS) of the Republic of Montenegro. Law on the Agency for National Security provides that the ANS authorized to secretly collect data by surveillance of the electronic communications and postal items (Article 9 paragraph 1 item 4 LANS MNE).

Surveillance of the electronic communications in the purpose of secretly collecting of data, on the base of written proposal from the Director of the ANS, in each case, must be approved by the decision of President of the Supreme Court of Montenegro, and in the case of his absence the decision will given by judge who replaces him in accordance with the law, if there are grounds for suspicion that threatened national security: 1) preparations for an armed attack on Montenegro; 2) covert activities directed against the territorial integrity of Montenegro; 3) covert activities, planning and preparing for the performance of the performance of internal and international terrorist attacks and other violent actions against state authorities and holders of public office in Montenegro or abroad; 4) providing classified information to unauthorized persons; 5) intelligence and subversive activities of individuals, groups and organizations for the benefit of other countries; 6) the organized criminal activity. Decision for application of surveillance of the electronic communications by ANS shall be made within 48 hours of the submission of the proposal (Article 14 LANS MNE).

Proposal for control of electronic communications contain information on the person to whom it applies control; the merits of the reasons for its use; the mode of administration; scope and duration; electronic means of the communication and circumstances that necessitate the need for this type of data collection. Surveillance of electronic communications pursuant to the Law of ANS application of this measure can take for three months, and for important reasons can be extended each time for another three months, or a total of not more than 24 months. Extension of application of this measure approving President of the Supreme Court of Montenegro, in the case of his absence decision will be made by judge who replaces him. Supervision of electronic communications shall be repealed immediately after the cessation of the reasons because it carried out. Director of the Agency, in writing, inform the President of the

Supreme Court of Montenegro, on the cessation of the reasons his inspection. Operators and providers of electronic communications services, as well as the Postal operators are obliged to provide the Agency and guarantee the conditions for supervision of electronic communications, which was approved by the President of the Supreme Court or a judge who replaces him (Article 15 LANS MNE).

5. Conclusion

It is unthinkable to prevent and combat terrorism and organized crime without the application of modern tools, methods and techniques such as special investigative measures, and modern information tehnologies. The introduction of specific procedures aimed at detecting and proving the acts of organized crime and terrorism in a more efficient way, which makes the arranging process to significantly deviate from the principles and traditional institutions of regular criminal proceedings. The focus of the proceedings is transferred to the earliest phase, instead of the criminal investigation, evidence actions are taken in preliminary investigation which is understandable reason because the later would not be effective or are by their nature such that they afterwards can not be taken, for example., interception, collection and recording of computer data of a suspect. Because of these there is need for implementation so-called proactive criminalistics investigation.

Preventive or proactive criminal investigations includes the undertaking of criminalistics measures, actions and resources in order to prevent the materialization of criminal intent, which tentatively, we can say that it is "real" (timely) criminalistics protection of society from severe forms of crime such as organized crime and terrorism. Thus, the full and effective protection of the desired state and the individual and collective sense of security requires displacement of criminalistics activities from reactive to proactive phase. The primary reactive and event-driven criminalistic investigation in the protection of society from severe forms of crime such as organized crime and terrorism, or the standard model of the organization of criminalistics activity, must be replaced by a proactive approach. The focus of this proactive approach is the timely identification of the potential holders of such criminal activities. This is possible only, by problem-oriented approach of criminalistics activity, which include a deep analysis of the causes, manifestations, dynamics and structure of certain types of crime. However, taking into account fact that a good portion of members of organized criminal or terrorist groups has no criminal record, *i.e.* not previously known to the police and security services, and that their criminal activity carried out in the framework of legitimate activities, problem-oriented approach in such cases can hardly lead to effective results, as a consequence requires a parallel application of criminalistic intelligence work as an effective response to criminal activity. In contrast to the problem-oriented approach in which the focus are the causes of crime problems, the focus of criminalistics intelligence work are the perpetrators. The criminalistics intelligence work mostly involves the monitoring of known and potential criminals, which is not limited to the investigation of specific crimes, but to gain insight into their criminal careers, lifestyle habits, it plans to be based on an analysis of these findings may perform pre-suppositions that could be useful for timely and effective preventative treatment.

From everything above we can conclude how should be proactive criminalistics investigation organized in regarding to knowledge management system. So we will

described it by giving the answers to question that we was nominate in this paper. The first question is which sort of knowledge is required for effective realization of this activity? Regarding to this question police need intelligence knowledge about criminal intentions of members of terrorist and organized criminal groups. Its required police (heuristic) activity and philosophy, which includes the process of collecting, analyzing and evaluating of the security interesting data for efficient crime prevention. It is more than previously gathered and processed by the information provided in the conspiratorial manner. Focus is on the conversion of data and informations into intelligence knowledge. Intelligence knowledge and thus enables decision-makers, to predict its further criminal behavior, and to choose the best solution for prevent it. This means that we need knowledge which giving answers on folows questions: Which criminal activity has been preparing? Which circumstance, relationship, process or activity produced the idea of the realization of a criminal activity that is being prepared? In what form and with what intensity will manifest? What are the possible *modus operandi* of offenders? Which values are threatened and what consequences can be caused? Who are the holders of the occurrence, or subjects of threat? In which area criminal activity will manifest?

Second question is how we can gathering that knowledge? That knowledge should be gathered in the phase of pre-materialization of criminal intent. Which mean in secrecy and by special investigative measures. Thus we come to the third question, what is it connection between obtaining of that knowledge and use of information technologies? The connection is Digital Forensics. With that we means use of knowledge from the field of Digital Forensic in application special investigative measure of interception, collection and recording of computer data, and in analysis of digital evidence which are provided by this special investigative measure. At the end there is question how knowledge management should be implemented in scope of proactive criminalistics investigation? And the answer is that that knowledge which is gather intelligence from criminogenic environment, and then analyze and interpret to determine which criminal activities are currently being implemented and who are the main holders (potential security risks and threats), must then be used to influence on the decision makers, to they promptly activate all available means for impact on all criminal activities that take place or preparing in a given criminogenic environment in order to prevent them. By this way criminalistics proactive investigation achieve both objective, prevention of committing the crime, and obtaining evidence for prosecution and punishment of carriers of preparatory actions or organized crime and terrorism.

In that sense special investigative measure of interception, collection and recording of computer data should have main role in proactive criminalistics investigation. Reason for this conclusion lays in fact that in comparation with the other special investigative measures prescribed by Criminal Procedural Code such as rendering simulated business services and conclusion of simulated legal affairs, enagagement of an undercover agent, controlled delivery, examination of cooperating witnesses..., implementation of this measure is almost always possible. Namely, why aplications of other special investigative measures is not always possible in every case of organized criminal and terrorism, application of measure of interception, collection and recording of computer data is almost always possible.

By the analysis of all of the above in respect of legislation concerning the application of special investigative measure of interception, collection and recording of computer data, we can conclude that the current legislation of the Republic of

Montenegro in a rather good way achieves a balance between the interests of the criminal proceedings or timely detection and prosecution of offenders of severe crimes such as organized crime and terrorism, on the one hand, and protection of personal rights and freedoms, on the other hand. Current legal provisions in the national legislation of Republic of Montenegro are introduced recommendation of Convention on Cybercrime from 2001st.

We can conclude that the legislation of the Republic of Montenegro makes a distinction between the interception of data that are generated in real time, while the signal passes through a computer network from source to destination communications, and preservation of stored computer data for the prevention and detection of criminal activity. Specifically, in terms of collecting data that are generated in real time, while the signal passes through a computer network from source to destination of communications, legislator is by provisions of the Criminal Procedural Code relating to the special investigative measure interception, collection and recording of computer data and the Law on Electronic Communications and Law on the national Security Agency predicted the possibility of real-time interception of computer data communications traffic and content data communications. Also, the provisions of the mentioned laws provides the obligation of preservation of stored computer data that could be crucial to the success of criminal investigations. The point of these activities is a sort of "freeze data" in order to prevent the loss or modification of existing data that could be of value prevention and detection of criminal activities, and that by order of the competent authorities carry out telecommunications service providers. We can also see that this action was limited duration (not less than six months but not longer than two years), and that this action is intended to preserve certain data and maintain their integrity, and that it can only refer the traffic data but not the content of communications.

At the end from all this we can conclude that is required strategic and planned approach in the application of knowledge of digital forensics in order to realize the knowledge driven proactive criminalistics investigations. In fact, to be able to apply special investigative measure interception, collection and recording of computer data, and to be able to get to the digital data by which analysis would get intelligence knowledge, first it is necessary to get to the grounds for suspicion that terrorist attack or an act of organized crime is preparing. This means that the focus criminalistics activities should be aimed at creating conditions for the implementation of these measure. Then, when it comes to digital data, it is critical to make their analysis in order to come to the knowledge by which we should predict their future behavior in terms of preparatory actions and materialization criminal intentions and also to prove it at the court. So if we implementation of mentioned special investigative measure will begin at the level of grounds for suspicion, then after its application we must reach beyond a reasonable doubt that certain people are preparing a terrorist attack or an act of organized crime, only then we have fulfilled the conditions for their arrest and bring to justice, by which is the goal of proactive criminalistics investigations fulfilled.

In this regard, knowledge management skills from the field of timely and adequately application of Digital Forensics within the proactive criminalistics investigations should be developed at personnel which are in charge for combating of the organized crime and terrorism, in a purpose to prevent it.

Future Research

According to the author it would be desirable in the future to perform research in the sense, in how many cases of detection and prosecution of organized crime and terrorism because of the preparatory activities for the execution of these crimes has been applied special investigative measure interception, collection and recording of computer data and how many of these cases ended with condemning verdict which was based on evidence obtained through this measure. Such research would certainly confirm the author's hypothesis that the timely implementation of these measures is crucial for the effective countering these forms of criminal manifestations.

References

1. Awad, E. M., & Ghaziri, H. (2004). Knowledge management (1st ed.). New Jersey: Prentice Hall.

2. Chang, W., Chung, P., (2014) Knowledge Management in Cybercrime Investigation – A Case Study of identifying Cybercrime Investigation Knowledge in Taiwan, Intelligence and Security Informatics, vol. 8440, 8-17. Retrieved from

3. Chen, H., Schroeder, J., Hauck, R.V., Ridgeway, L., Atabakhsh, H., Gupta, H., et al. (2002). COPLINK connect: Information and knowledge management for law enforcement. *Decision Support Systems, 34,* 271–285. Retrieved from

4. Criminal Procedural Code, Official Gazette of MNE ", No. 57/09 of 18 August 2009.

5. Dean, G., Fahsing, I. A., Glomseth, R., Gottschalk, P., (2008). Capturing knowledge of police investigations: towards a research agenda, *Police practice and Research, vol. 9, no. 4.*, 341-355. Retrieved from

6. Dvoršek, A., (2008) Criminalistics strategy, University of Maribor, Ljubljana: Faculty of Criminal Justice and Security.

7. Dvoršek, A., (2009) Criminalistics intelligence work and its perspectives in criminalistics, Conference proceedings: Law and Forensics in criminalistics, Criminalistics-Police Academy, Belgrade, 46-52.

8. Fasihuddin (2008). Identification of Potential Terrorism: The problem and implications for Law-enforcement in Pakistan, International Journal of Criminal Justice Sciences (IJCJS), Vol 3 (2): 84–109. Retrieved from

9. Goldstein, H., (1979). Improving policing: A problem-oriented approach. Crime and Delingquency 24, 236-258.

10. Gottschalk, P., (2007). Knowledge Menagement System in Law Enforcement, Technologies and Technigues, London: Idea Group Publishing. Retrieved from

11. Irons, A. Ophoff, J. (2016). Aspects of digital forensics in South Africa, Interdisciplinary Journal of Information, Knowledge, and Menagement, 11, 273-283. Retrieved from

12. Ivanović, A., Faladžić, A., (2011) The application of special investigative measures in detecting and prosecuting organized crime and terrorism, Conference proceedings: Policing in central and eastern Europe – Social control of unconventional deviance, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, 331-350. Retreived from

13. Ivanović, A., Munižaba, B., (2013). Application of principles of organization and methodology of criminolistics in the protection of national security, Proceedings of the

scientific conference: Place and perspectives of criminalistics, criminology and security studies in modern terms, Faculty of Criminology and Security Studies, University of Sarajevo, Sarajevo, 97-103. Retreived from

14. Järvenpää, E., Kopra, M-J., & Lanz, M. (2016). Challenges of knowledge and information management during new product introduction: Experiences from a Finnish multinational company. Interdisciplinary Journal of Information, Knowledge, and Menagement, 11, 285-308. Retrieved from

15. Klink, M., Kordus, S., (1986). *Kriminalstrategie: Grundlagen polizeilicher Verbrechensbekämpfung*, Stuttgart: Boorberg.

16. Lahneman, W. J. (2004). Knowledge-sharing in the intelligence community after 9/11. *International Journal of Intelligence and Counterintelligence*, 17, 614-633.

17. Law of Electronic Communications, Official Gazette of MNE no. 01-1452 / 2 from 2013

18. Law on the Agency for National Security, Official Gazette of MNE no. 20/2011.

19. Luen, T.W., & Al-Hawamdeh, S. (2001). Knowledge management in the public sector: Principles and practices in police work. *Journal of Information Science, 27*(5), 311–318.

20. Rakočević, V., (2014). Special investigative methods, Podgorica: Faculty of Law.

21. Srinivasan, S., (2012). Digital forensic curriculum in security educaton, Jurnal of Information Technology Education: Innovations In Practice, 11, 147-157, Retrieved from

22. The Criminal Code of Montenegro, Official Gazette of MNE no. 70/2003, 13/2004, 47/2006 and Sl. Gazette of MNE no. 40/2008, 25/2010, 32/2011, 40/2013 and 56/2013, and 3/15.

23. Weisburd, D., Telep, C., Hinkle, J., Eck, J., (2008) *Effects of Problem-Oriented Policing on Crime and Disorder*, New York: U. S. Department of Justice,

24. Wolfe, B. H., An Introducton to computer forensics: Gathering Evidence in a Computing Environment, Informing Science: *The International Journal of an Emerging Transdiscipline (InformingSciJ) - Special Series: Expanding the Focus*, vol. 4. no. 2, 47-52. Retrieved from