FIGHT AGAINST ORGANISED CRIME AND SOME CONTEMPORARY CRIMINALISTICS METHODS[1]

Branko Leštanin
Ministry of the Interior of the Republic of Serbia

Željko Nikač, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Abstract: The paper gives a brief overview of the definition of organized crime with the answer what definition is most appropriate from the aspect of police work. The basic characteristics of organized crime are also presented. In the continuation, the paper gives an overview on some methods used by members of an organized criminal group or criminal organization as a whole in order to obscure their criminal activities and avoid criminal prosecution. An analysis of the practical activities of the police and modern technologies reveals certain possibilities that can lead to the improvement of police work in the field of the fight against organized crime. An analysis of the content of available literature related to the topic of paper was also carried out. To improve the rates of detecting and clarifying of organized crime, police must primarily be able to assess the perpetrators of such crimes. Finally, the synthesis of all methods leads to the conclusion what methods are the most effective. All contemporary methods have to be used while respecting the fundamental rights and freedoms that are guaranteed by the constitution and international legal acts. If not so, all police and prosecutor work on proving the felonies will 'go down the drain' as the courts must declare the evidence to be inadmissible and unlawful.

Keywords: organized crime, contemporary methods, mobile phones, i2 analysis, drones.

INTRODUCTION

Organized crime of the modern era has introduced completely new forms and types of criminal behavior, characterized by new ways of perpetrating the felonies, which causes great (material and non-material) damage to the community.

1 The paper is the result of work on the project on the *Development of Institutional Capacities, Standards and Procedures for Combating Organized Crime anda Terrorism in the Conditions of International Integration*, conducted by MPNTR No.17904.

An essential characteristic of the criminal acts of organized crime is reflected in the increasing need for covert resolving and proofing because perpetrators, as members of organized criminal groups, use modern technical achievements. An additional problem is the lack of legal regulations, non-equal judicial practices, outdated criminal-intelligence methods and the lack of professional staff to monitor this kind of organized crime. Drug trafficking, illegal dealing in weapons, kidnapping, extortion, cybercrime, corruptive offenses can be distinguished as the most serious forms of organized crime.

In scientific and professional circles there are various theoretical definitions of the concept of organized crime, its characteristics and elements. Regarding the fulfillment of the conditions for the existence of felonies in the field of organized crime, the established conditions laid down in the UN Convention against Transnational Organized Crime (Palermo Convention) should be respected, and the provisions of the national criminal legislation of most states are harmonized with it. According to Nikač and Božić (2018) it is necessary to accept an extensive interpretation, according to which organized crime is an organized criminal activity by a criminal organization with a properly established hierarchy of relationships, division of labor, network structure, methodology of action which implies systematicity, conspiracy, corruption and connection with parts of state structures with the aim of achieving extra profits, avoiding criminal responsibility and legalizing criminal proceeds. From the police point of view, the most important are the elements prescribed by the national criminal legislation, as it is directly enforced by police officers[2].

The most important characteristics of organized crime that stand out include:

1. Specific network organization;
2. Clear "deal of business" both in the criminal organization itself and between criminal organizations;
3. Strict subordination relationship;
4. Loyalty and solidarity of members of a criminal organization;
5. Family morality elements;
6. 'The law of silence' (*omerta*);
7. Criminal activity planning;
8. Specialization of members of a criminal organization;
9. Terrorism and organized crime nexus; and
10. Use of violence and intimidation.

The most famous criminal organizations in the world have been distinguished and they include: the Italian mafia (*Cosa Nostra, Camorra, and N'drangheta*), Albanian mafia, Russian mafia, Chinese Triad, Japanese Yakuza, Colombian and Mexican cartels, Nigerian organization and numerous US criminal organizations[3].

2 Further readings in Božić, Nikač, Simić, 2017:273-276
3 Further readings in Nikač, 2014:135-158

The aim of this paper is to give an overview of some methods used by members of an organized criminal group (OCG) or criminal organization as a whole in order to obscure their criminal activities and avoid criminal prosecution. An analysis of the practical activities of the police and modern technologies reveals certain possibilities that can lead to the improvement of police work in the field of the fight against organized crime. Finally, the synthesis of all methods leads to the conclusion what methods are most effective.

MOBILE PHONES AND ORGANIZED CRIME

In the first place, in the collection of data on organized crime, the criminal intelligence policing are set up, where, using informants and other operational methods, data on the criminal activity of a particular criminal organization and its members have to be collected. Various contemporary technical accomplishments can help members of OCGs in committing the crimes that allows them greater motion and mobility, so it is one of the essential characteristics and a few examples will be given to illustrate the monitoring of these activities.

In order to avoid 'linking' by monitoring the listing (records) of mobile phones, or secret surveillance of communication, perpetrators use the so-called 'specials' i.e. mobile phones and SIM[4] cards that only serve to commit a felony and use during the commission of it. To improve efficiency in identifying the numbers of SIM cards, the law enforcement agency could use software that can identify unknown calls and messages. That kind of software (apps) can be downloaded from web stores (Windows, Google, Apple) for free and be useful tool for analyzing the communication between perpetrators. As an example, it can be listed as one of the following: Everybody, Truecaller, NumBuster, CallClerk, Saller ID Spoofer, etc.

It has been noticed by law enforcement officers that mobile phones appeared with the so-called 'cracked' and 'cloned' IMEI[5] number that is very difficult to track and which is used by the perpetrators not only of these, but also of other crimes. Often perpetrators also own several mobile phones and SIM cards (usually prepaid) and if they suspect that there is a possibility of discovery, they throw mobile phones and cards in separate places to cover up any trace. To avoid the so-called 'regular' communication via calls or SMS messages, perpetrators use social networking services such as Facebook, Viber, Skype, WhatsApp, Twitter, LinkedIn, Flickr etc. (Leštanin, 2017:299). However, in this type of communication, it is specific that it is necessary for the phone to be connected to a wireless (Wi-Fi) internet or mobile internet data exchange in order for the software application to function. Recently the Viber and WhatsApp have introduced the 'end-to-end'

4 Subscriber Identity Module

5 International Mobile Equipment Identity; 'Cracked' IMEI is actually changed, falsified, fake number with software which shows that one mobile phone device has several IMEI numbers. These IMEI numbers are also used by some other mobile phone devices that do not have anything in common with perpetrator(s). 'Cloned' IMEI speaks for itself that there are two mobile phone devices with the same IMEI number.

encrypted system between participants in conversation that disables the possibility to intercept it. This kind of obstacle probably could be overcome by some encryption software.

To overcome this, law enforcement could use the stingray devices or/and IMSI[6]-catchers (or just a Catcher) contemporary technical devices that can track all communications (phone calls, SMS messages, emails and communications via all kind of messengers) nearby. Basically the Catcher represents the 'fake' cell tower (base station) acting between the mobile phone that is targeted and the service provider's real cell towers. Mobile phone always chooses the cell tower with the strongest signal which is this case the Catcher. Metaphorically speaking, the Catcher is like a 'sponge' for mobile phone waves. In professional cycles there are rumors that alternative communications by all kind of messengers, electronic mails and so on can be followed with these devices.

The biggest controversy, from the fundamental rights and freedoms aspects, is the fact that the Catcher device monitors all communications that take place over the cell tower and not just the target's communication. It is therefore necessary that the court warrant for the using of this device be clear and precise, with the obligation to delete data from other non-targeted communications. Some preliminary research has been done in trying to detect and frustrate Catchers. One such project is through the Osmocom open source mobile station software. This is a special type of mobile phone firmware that can be used to detect and fingerprint certain network characteristics of Catchers, and warn the user that there is such a device operating in their area. But this firmware/software-based detection is strongly limited to a select few, outdated GSM mobile phones (i.e. Motorola) that are no longer available in the open market. The main problem is the closed-source nature of the major mobile phone producers (*https://en.wikipedia.org/wiki/IMSI-catcher#cite_ref-20*). Several apps listed on the Google Play Store as Catcher detector apps include SnoopSnitch, Cell Spy Catcher, and GSM Spy Finder and have between 100,000 and 500,000 app downloads each. However, these apps have limitations in that they do not have access to phone's underlying hardware and may offer only minimal protection (*https://motherboard.vice.com/en_us/article/neeb5g/stingray-detection-apps-might-not-be-all-that-good-research-suggests*).

IPhones are a special issue for detecting the communication between the crime perpetrators. The iPhones have six-digit passwords which are used to access them. Additionally the iOS operating system has own apps for audio/video calls and messages communication. For audio/video calls it can be used Face Time app and for messages iMessage app. The main precondition is that a device must be on wireless or mobile data exchange network. The Apple Inc. does not want to help law enforcement (above all the FBI) to crack it open. In 2015 and 2016, Apple Inc. has received and objected to or challenged at least 11 orders issued by US district courts under the *All Writs Act* from 1789. Most of these seek to

6 International Mobile Subscriber Identity

compel Apple 'to use its existing capabilities to extract data like contacts, photos and calls from locked iPhones running on operating systems iOS 7 and older' in order to assist in criminal investigations and prosecutions. A few requests, however, involve phones with more extensive security protections, which Apple has no current ability to break. These orders would compel Apple to write new software that would let the government bypass these devices' security and unlock the phones (*https://theintercept.com/2016/02/23/new-court-filing-reveals-apple-faces-12-other-requests-to-break-into-locked-iphones/*). The use of the *All Writs Act* to compel Apple to produce new software was unprecedented and, according to legal experts, it was likely to prompt 'an epic fight pitting privacy against national security' (*http://www.latimes.com/business/la-me-fbi-apple-legal-20160219-story.html*). It was also pointed out that the implications of the legal precedent that would be established by the success of this action against Apple would go far beyond the issues of privacy (*https://www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case*). The FBI vs. Apple Inc. case did not end before a court because FBI announced that the device had been cracked. In any case, other law enforcement agencies will follow the example of FBI.

Whatever type of mobile phone appears to be used for the purpose of a perpetrator's communication, in order to get into its content and to extract the contacts, recorded calls, messages, images or anything else the law enforcement officers and prosecutor will need a court warrant. This procedure is considered as the special investigative procedure of computer data search although the mobile phone and computer are different devices. Regardless of this, contemporary mobile phones have most of the computer functions (storing the video and image, emails, social networking, links to cloud storage, storing all kind of data, etc.). For that reasons, in a broader sense, this procedure could be considered as computer data search.

For analyzing the mobile phone's data and other intelligence, police use the so-called 'i2' analysis. The first products included the i2 Link Notebook and i2 Case Notebook. The *i2 Link Notebook* enabled investigators to create entity relationship diagrams (a kind of visual database) allowing raw intelligence – largely textual reports (e.g. witness statements) – to be entered manually, revealing the relationships within the data and enabling data from different sources to be collated and graded. Automatic and manual layouts, and the ability to create, share, search, analyze and, most importantly, print, even extremely large charts (sometimes tens of meters in length), dramatically improved law enforcement's ability to understand and communicate the status of investigations, and to direct and manage the process. The *i2 Case Notebook* provided similar data entry and visualization of time series data (i.e. laying events out along themes such as people and places), allowing once again the law enforcement officials to handle very large data sets. Even with variable density timescales, due to the very large number of events uncovered in a large investigation, a single Case Chart could cover several walls in an office, or stretch tens of meters along a corridor (*https://en.wikipedia.org/wiki/I2_Limited*).

In terms of communications, the i2 analysis helps law enforcers to analyze recorded communication between perpetrators and, concretely, to establish from which telephone numbers perpetrators communicated, how many times, for how long, what base stations they used, what their relationships are, and many other information (Image 1). It can also connect all other data from intelligence reports, statements, notes regarding the perpetrators, and so on. What must be emphasized is that not every police officer can work in i2. Only the well trained analysts can operate this complex software. The end result could be the most important finding for the criminal proceedings.

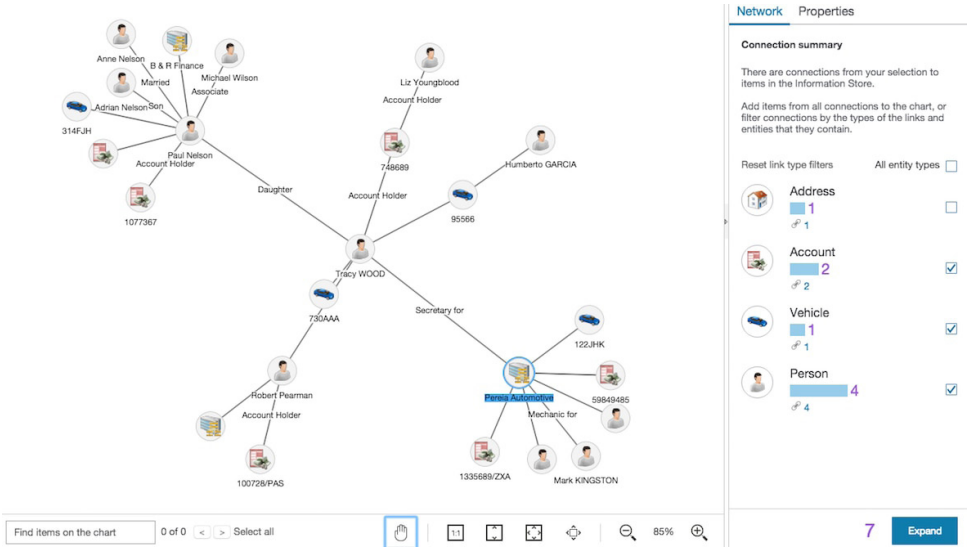

Image 1 – i2: *analysis software application report*
(source: https://www.ibm.com/us-en/marketplace/enterprise-intelligence-analysis)

DRONES IN POLICE WORK

Talking about monitoring, this primarily refers to secret surveillance and perceiving or undercover operations as 'operative' police procedures, and not to secret monitoring and recording as special evidentiary procedures from Criminal Procedures Code (CPC). Before there is a basis for suspicion or a sufficient set of facts, police officers may collect information and data aiming to determine whether they have acquired the basis of suspicion that a felony or misdemeanor has been committed. Collecting data and information is done through secret and direct observation–scanning or observing persons, objects, means of transport and space, but only for the purpose of checking the received information or knowledge (indications) and forming a proposal to the competent authorities for which they are authorized by the CPC (Djurdjević, Radović, 2017:108). This procedure is undertaken with the aim of collecting information on persons

and groups dealing with organized crime, primarily information on the place of residence, work, data on business friends, friendly and other relationships, information on propensities and habits, and in particular information on location of secret hiding places and shelters, information on intermediaries and resellers, on how to transfer and conceal goods, discover the source of goods and discover the organizer and the main bearers of such activity. The main purpose of doing this is to find the items or goods in order to provide material evidence for further criminal procedure. Further, for the purpose of monitoring the movements of perpetrators in their vehicles, the GPS devices could also be used. This is essential when police want to find hidden storages with illicit goods. The processes of placing a GPS device on the vehicle and removing it must be strictly confidential, quick and in accordance with the CPC.

In addition, the police can use an unmanned aircrafts-UA[7] to reconnaissance the terrain or monitor the movement of perpetrators. It must be emphasized that the use of drones could violate the air space of another state. To overcome this problem the states and their police must arrange the using of drones reciprocally. The advantages of drones that the police can use are that they are small, relatively fast, offer the possibility of day and night surveillance (recording), have the silent mode, provide extensive coverage of the observation area, make it possible to capture a perpetrator at the crime scene, etc. The use of drones is not always possible; because of this, it is always necessary to assess the configuration of terrain and climatic (atmospheric) conditions (e.g. closely-set buildings, a large number of wires in the area of drone movement, dense trees, the strength and direction of the wind, possible rainfall, fog-visibility, etc.). Using drones must be pursuant to the legal framework and without violations of rights and freedoms of citizens. If there is reasonable doubt that criminal evidence will be collected using a drone or that the usage will intrude upon reasonable expectations of privacy it must be used with a court warrant. Except when used on a warrant by the criminal court, the use of UAs must include some controlling (supervising) mechanism too. A drone's footages can be evidence in the criminal court in the case where a court warrant was previously issued.[8]

The IACP[9] even suggests that police should engage their community early in the planning process, including their governing body and civil liberties advocates. The community should be provided an opportunity to review and comment on agency procedures as they are being drafted. Where appropriate, recommendations should be considered for adoption in the policy. As with the community, the news media should be brought into the process early in its development (Aviation Committee of International Association of Chiefs of Police, 2012:2).

7 Unmanned aerial vehicle (UAV), Remote Piloted Aircraft (RPA) or simply a drone
8 Further reading in S.C. Schwartz, 2017
9 International Association of Chiefs of Police

SOME OTHER METHODS

Special emphasis must be placed on the fact that a trend has been noted in Serbia where crime perpetrators communicate using handheld radio devices (walkie talkie) that are easily accessible in any store and are difficult to survey by the law enforcement agencies (Leštanin, 2017:299). We think it is very difficult to put these devices under surveillance because they work on various frequencies, they sometimes can only be dual, they do not have the need for base stations as mobile phones, they are difficult to locate, etc. As a result, it is very easy for the perpetrators to avoid prosecution using the radio or to prevent the detection of other offenders. However, this can be achieved through a well-planned inquiry and possibly using an undercover policeman.

It has been noticed lately that well organized transnational criminals use draft emails. They create an account on a free email provider's web (Gmail, Yahoo, Hotmail, etc.) that does not contain any personal data of actual owner in order to avoid detection. Through that account they neither send nor receive any emails but they only write drafts and save these on the account. Both sides in conversation have a password of that account and use it for accessing. In this manner they avoid email going through network and being tracked or intercepted. For law enforcement it is one more task to be accomplished if they want their counter-crime operations to be efficient and effective.

Cloud storages are a special story, too. Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the Internet with pay-as-you-go pricing. With cloud computing, you do not need to make large upfront investments in hardware and spend a lot of time on the managing of that hardware. Instead, you can be provided with exactly the right type and size of computing resources you need to power your newest bright idea or operate your IT department. You can access as many resources as you need, almost instantly, and only pay for what you use (https://aws.amazon.com/what-is-cloud-computing/). These opportunities can be abused by criminals in order to store data in storages that are necessary for their criminal activity. They can also be used for data exchange and communication regardless of where criminals are.

All of these special investigative techniques must be pursuant the law. Speaking in terms of Western Balkan countries, it is CPC. It is especially important that everything is done in accordance with the norms of the Constitution and laws (Codes) and respecting the fundamental rights and freedoms guaranteed in them. Essential for the performance of these procedures is a court warrant, but not just any warrant. The warrant must specify the reasons for the court ruling on such a decision and justifying the lawful violation of the guaranteed rights and freedoms (the right to private life, the right to freedom of movement and so on)[10].

10 Further readings in Marinković, 2010

When communicating between themselves, perpetrators try to use pre-arranged codes to avoid detection if their mobile phones or radio are surveyed or monitored. Here, we are faced with the creativity of the perpetrators who invent various codes, for example, for police officers, for police vehicles, for the police building, for the warehouses where they store their illicit goods or the vehicles used during the commission of the felony, as well as the specific nicknames they give to one another during the commission of the felony, which are only known to them (Leštanin, 2017:299). Practice points to the following: suspects use encryption for communication; the result of the application of special investigative procedures surveillance and technical recording of telecommunications is a very small number of relevant communications; police officers carrying out this special investigative procedure do not conduct adequate analyses of intercepted telecommunications; in Bosnia and Herzegovina, an expert is not engaged in criminal proceedings who would, through the use of their knowledge and skills for the purposes of criminal proceedings, conduct an analysis and interpretation of encrypted intercepted telecommunications. Bearing in mind the fact that the above operation and the technical recording of telecommunications can be carried out for a relatively long period of time (up to 6 months) and that as a final outcome of its implementation we have a small number of relevant communications, it would be inadmissible for this small sample to be 'spent' in an inadequate manner at the main trial (Vujić, Zimonja, 2017:103).

Finally the criminals have to communicate in order to make arrangements about how to carry out the felony. The major task for law enforcement agencies is to find the way how to intercept this communication.

Well-organized OCGs use the so-called (in police jargon) 'cleaners'. These are the aiders who observe the way of moving vehicles with illicit goods, the movement of police patrols, police buildings and other interesting personalities and phenomena. If they notice anything suspicious, they have a task to inform either the organizer or the person directly transporting the illicit goods to avoid contact with the police, customs, etc. In this sense, two types can be distinguished: *static and dynamic* 'cleaners'. The static 'cleaners' are those who observe one or more locations or movement of law enforcement from one place or just static objects. The dynamic 'cleaners' are those who use some means of transportation (a vehicle, a motorbike, a bicycle, etc.) and who, while on the movement, observe a certain part of the terrain and inform about the suspicious events. The term 'cleaner' was created in the 90's because the term 'clean' was used purely as a code confirming that there are no police patrols on the way of movement of illicit goods. According to some intelligence, this coded term is still used in Serbia. They pay special attention to shifts handover between police officers so that they should move right at the time of handover when police officers are not expected to be able to detect and arrest them.

Criminals often use decoys to avoid police ambushes. The perpetrators of crime found out that police officers in the police ambush let through the 'clean-

ers' going in front of the vehicle with the goods and then stopped only the vehicle with goods and arrested perpetrators. In order to avoid this, the organizers send no more than a few vehicles – decoys (usually a van or a small truck) which is acting in the transport of goods. If they are stopped, no goods are found since these vehicles are empty, so that no arrests can occur. In order to avoid this kind of embarrassment, police officers have to prepare a police ambush well and collect intelligence about all vehicles, about the exact vehicle that transports goods, to find out the beginning of the movement of the vehicle with the goods, to pay attention to a vehicle (the truck/van with the goods moves slowly, its motor is buzzing, tires and buffers are lower than usual, etc.).

Great adaptability to the situation and movement on the market is another important feature of the perpetrators of these crimes. They have knowledge about where and what kind of goods are prohibited or restricted (e.g. basic provisions for human life, goods of wide consumption, etc.) and how to avoid to be spotted by law enforcement officials. Prices of certain goods vary depend on supply and demand and other economic factors. Therefore, the perpetrators can quickly change the type of goods that are the subject of felony, which only indicates the level of professionalization and specialization of the perpetrators. Regardless of the changes in the types of goods, the perpetrators do not change the modus operandi, the established routes of movement on which they have not been discovered, the members of the group, and all other circumstances related to the commission of felonies. Only the change of end customers and users of certain illicit goods can occur, as consumers are different. What is particularly dangerous with these perpetrators is the possibility to easily pass from the smuggling of weapons and drugs into the sphere of terrorism. In police practice, there were indications that certain criminal groups engaged in illicit trade were switching to the smuggling of drugs, weapons and aiding terrorists. However, these indications have not been confirmed through the policing in practice.

As for the personality of a person involved in organized crime, these are people are, as a rule, very intelligent, skillful, very communicative and mobile, but at the same time very cunning, ingenious and resourceful, yet also very perfidious and without much scruples (Djošić, 1970:43). They do not keep their goods in their homes or apartments, there are already rented 'stacks' and hidden warehouses where goods are stored and which very few people know of. The organizers of the 'business' are very cautious and cooperate only with already known and tried associates (buyers/sellers) and a 'new player' can enter the job only on the recommendation of a confidential one. The new arrivals are often thoroughly checked in order to establish who are they, what they did before, what the members of the family are doing, etc., as well the put on a test through scheduling multiple meetings in different places, giving smaller quantities of illicit goods, tendentious arrest and disclosure by the police, and so on.

They are often prone to fleeing both in the course of and after arrest, as well as to offer resistance and launch attacks on police officers in order to avoid capture

and responsibility for crime and possibly hide the tracks and evidence which may lead to them. On the other hand, if they find it convenient, they do not hesitate to offer money or any other gift to police officers or other persons involved in suppressing this phenomenon (inspections). In community, they are perceived as being gallant and cavaliers and tend to give the impression of people with nice manners, and when they are caught in the illegal business they usually try to make a 'legend' that they are not guilty; they almost never admit committing of a crime and will frequently put up an act of a naive and honest man, etc. They often help the local community where they have hidden storages, where they exchange money and goods, on the ways where they transporting the goods, etc. Helping implies giving the money, taking care of lone and old members of family, giving some basic means for living, housekeeping, etc.

In clashing with the competition and in order to achieve the material gain from felonies, they do not refrain from using the worst threats, blackmail and fraud (Djošić, 1970:43). It is not uncommon for perpetrators to offer 'cooperation' to police officers, but they must be particularly careful not to become involved in their traps aimed at destroying the criminal competition and taking a 'monopoly' over an illegal market. By belonging to this group of people and moving in these circles, police officers can directly come to the knowledge when they are preparing to commit or arranging the perpetration of a felony or some other criminal activity. A police officer must be smart enough and able to visualize the true motives of criminals who gives him/her information so that there is no abuse of police protocols (rules).

CONCLUSION

Organized crime groups are specialized in perpetrating felonies and most of them are professionals. Severity of felonies in Western Balkan countries is considered differently due to varying criminal-law aspects. In this sense, their respective police authorities involve different resources in detecting and clarifying them. For that purpose members of OCGs also use contemporary techniques and devices which put them a 'step forward' in respect of the state authorities.

To improve the detecting and clarifying rates of organized crime, the police must first assess the resources of both perpetrators and the police force. When they are assessing the perpetrators, the police have to gather useful intelligence referring to their personal data, family members, apartments, houses, storages, vehicles, legal or illegal firearms, associates, places of gathering (pubs, restaurants, hotels, etc.), means of communication (personal computers, tablets, laptops, cell phones, radio, etc.) and all other intelligence that is important for assessing the perpetrators. For efficient assessment of police forces, it must be known what their resources are (human, vehicles, communications, etc.), if they need extra resources, whether they have trained officers or enough human and technical

means to enforce the operations. After assessing both sides, the operations can be planned and carried out.

Taking into account that OCGs are well organized in the region of the Western Balkans, the police should, together with the prosecutor, investigate these felonies with special evidentiary procedures and applying special contemporary techniques and devices. But one very important fact must be on their mind. All measures and techniques have to be taken with due respect of fundamental rights and freedoms that are guaranteed by the constitution and international legal acts. If not, the police and prosecution's work on proving the felonies will 'go down the drain' since the courts must declare the evidence inadmissible and unlawful.

One of the main tools is the contemporary method of analyzing the intelligence data; exchange of intelligence between state authorities (in and out of state) and special investigate techniques. Using such tools, the police and prosecutors can do their job competently and improve detecting and clarifying rates of these felonies. In future, if the countries want to have successful investigation of organized crime and all other forms of crime they will have to undergo de-politicization of all state authorities that deal with crime issues.

REFERENCES

1. Aviation Committee of International Association of Chiefs of Police (2012), *Recommended Guidelines for the Use of Unmanned Aircraft*, IACP, https://www.theiacp.org/sites/default/files/all/i-j/IACP_UAGuidelines.pdf. Accessed on May 3, 2019
2. Božić, V., Nikač, Ž. (2018). Fight against Organized Crime in the States of the Region and EU Member States. In: Thematic collection of papers *Asymmetry and Strategy*, Strategic Research Institute & National Defence School, 342-343
3. Božić, V., Nikač, Ž., Simić, B. (2018). Fight Against Organized Crime with Reference to Permanent Education of Police Officers. In: Thematic conference proceedings *Policija i pravosudni organi kao garanti slobode i bezbednosti u pravnoj državi,* (2):271-290
4. Djošić, M. (1970). *Kriminalistička obrada krivičnih dela nedozvoljene trgovine*. Belgrade: Federal Secretariat of Interior, (internal printing)
5. Djurdjević, Z., Radović, N. (2017). *Kriminalistička operativa*, 3rd edition, Belgrade: Academy of Criminalistics and Police Studies
6. Leštanin, B. (2017). Criminal Law and Criminalistics Aspects of Illicit Trade as Criminal Offence. In: Thematic conference proceedings *Policija i pravosudni organi kao garanti slobode i bezbednosti u pravnoj državi,* (2):291-308
7. Mariniković, D. (2010). *Suzbijanje organizovanog kriminala-specijalne istražne metode*. Novi Sad: Prometej

8. Nikač, Ž. (2014). Initial Experiences in Combating Organized Crime in the World and in the Republic of Serbia. In: **Suprotstavljanje savremenom organizovanom kriminalu i terorizmu (5)7:135-158**
9. Schwartz, S.C. (2017). *Big Brother or Trusted Allies? How the Police Can Earn Community Support for Using Unmanned Aircraft*. Master thesis. Monterey, California: Naval Postgraduate School
10. Vujić, D., Zimonja, O. (2017). Dokazna vrijednost šifrovanih poruka iz presretnutih telekomunikacija u krivičnom postupku, *Criminalistics theory and practice* 4(7):91-105
11. UN Convention against Transnational Organized Crime, United Nations, Treaty Series, vol. 2225
12. https://aws.amazon.com/what-is-cloud-computing/. Accessed on May 2, 2019
13. https://en.wikipedia.org/wiki/IMSI-catcher#cite_ref-20 Accessed on May 1, 2019
14. https://en.wikipedia.org/wiki/I2_Limited. Accessed on May 2, 2019
15. https://motherboard.vice.com/en_us/article/neeb5g/stingray-detection-apps-might-not-be-all-that-good-research-suggests. Accessed on May 1, 2019
16. http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf. Accessed on May 2, 2019
17. https://theintercept.com/2016/02/23/new-court-filing-reveals-apple-faces-12-other-requests-to-break-into-locked-iphones/. Accessed on May 1, 2019
18. https://www.ibm.com/us-en/marketplace/enterprise-intelligence-analysis. Accessed on May 2, 2019
19. http://www.latimes.com/business/la-me-fbi-apple-legal-20160219-story.html. Accessed on May 1, 2019
20. https://www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case. Accessed on May 1, 2019