Paweł Łabuz, Ph.D.
adjunct in School of Economics, Law and Medical Sciences in Kielce
Tomasz Safjański, Ph.D.
WSPiA University of Rzeszów, VISNA Business Support Center

Counter-detection activities of criminal groups aimed at limiting the effectiveness of operational and procedural control and interception of conversations

Summary

The article presents the essential aspects of tactics and techniques applied by criminals with an aim to reduce the effectiveness of procedural eavesdropping and operational control. The most significant methods of protecting criminal correspondence were characterized. The above issues are exceptionally complicated, owing to the specifics of the activities to be discussed. To date, counter-detection activities of criminal organizations have not been within the main area of interest for forensics. The article highlights the benefits resulting from the knowledge of criminal tactics and techniques used to ensure the confidentiality of correspondence, in particular, in view of the ongoing legislative work pertaining to prosecutorial control exerted over operational and exploratory activities.

Keywords: procedural eavesdropping, operational control, counter-detection activities, criminal tactic

Introduction

Counter-detection activities discussed herein include any operations undertaken by individuals/groups engaged in any forms of criminal activity, aimed at ensuring the secretiveness and confidentiality of correspondence. Nowadays, the above activities include a wide spectrum of forms, methods and measures, which can be classified according to various criteria. In practice, these are the different measures of impeding or preventing law enforcement authorities from gathering information about the users of telecommunication devices, message contents, location data (data indicating the geographic position of the terminal device), time and place of correspondence, interlocutors, and, consequently, from collecting and securing evidence.

The criminals have for a long time recognized the benefits stemming from protecting their own correspondence. From the tactical and forensic point of view, such a protection is conditioned by limiting the effectiveness of the procedural eavesdropping and operational control. Consequently, the persons being subjected to such methods undertake various counter-detection activities, e.g. camouflaging, masking, legending and disinformation activities.

The essential objectives of operational control and procedural eavesdropping are consistent and aim at detecting and obtaining evidence of a crime. The legislative application of operational control (operational and procedural eavesdropping) in the course of detection activities was pre-determined by its high cognitive value and efficiency in fighting crime.

The doctrine emphasizes a problem of competition between the procedural eavesdropping and operational control. Unpublished statistical data confirm a clear advantage of operational control applied by the police and special services. However, it appears that both measures, used to detect crime and preserve evidence, should be perceived as complementary to each other. The scope of criminal cases involving the use of both methods is slightly different, which, at least in some cases, creates an opportunity to perceive operational eavesdropping as a subsidiary of procedural eavesdropping (Bożek, 2015).

Procedural eavesdropping and operational control

Due to implementation and exploitation related issues, the procedure of controlling and recording conversations, most commonly referred to as the procedural eavesdropping, is regulated only by the provisions of the Penal Code, and not by the acts setting out the competences of services authorized to use wiretaps in the course of operational and exploratory activities. The situation of duality as it pertains to clandestine control and recording of conversations, can, when a proper investigative tactic is adopted by a prosecutor, be exploited to extend the period of application of operational control of a person, or - after obtaining operational control recordings as evidence to be used in pre-trial proceedings - to subject this person to procedural eavesdropping.

Operational control is a method within a range of operational and exploratory activities and it consists in clandestinely monitoring the content of the correspondence, checking the contents of the shipments and applying technical measures which allow obtaining information and evidence in an implicit manner, in particular the contents of telephone conversations and other information transmitted via telecommunications networks. In practice, it comes down to the possibility of applying operational measures in relation to a wide range of methods of communication, the transfer of content or objects between parties.

The essential powers concerning the application of operational control are conferred under the acts of law setting out the services' competences[1]. Currently, nine state institutions are authorized to use operational control, including Police, Border Guard, Central Anticorruption Bureau, Internal Security Agency, Military Counterintelligence Service, Military Police, National Treasury Administration, Foreign Intelligence Agency, Military Intelligence Service.

As a rule, the above institutions may apply operational control in the course of operational and exploratory activities. Operational control can deliver various types of information, e.g. the contents of the telephone conversations (including those transmitted over mobile phone networks), texts, text messages, faxes, TV pictures, or even delivered by email or obtained through direct eavesdropping (installed in places inaccessible to the public) (Herzog, 2007).

Operational control allows collecting information about criminal activity prior to the initiation, during, or after completion of a criminal proceeding, in such a manner that it can be used as evidence. On the grounds of the aforementioned acts setting out the services' competences, the legislature opted to give the information gathered in the course of operational control the status enabling the initiation of a criminal proceeding or relevant to the already initiated proceeding. In practice, these materials are submitted to the Prosecutor's Office as annexes to the notification of a suspected criminal offense, and thus treated as evidence in criminal proceedings (Mąka, 2011).

Among the bodies authorized to conduct operational and exploratory activities are both those competent[2] and incompetent[3] to handle pre-trial proceedings. Under the laws governing the functioning of these bodies, they have general competence to perform operational and exploratory activities (Kaczorkiewicz, 2014). However, information concerning an offence falling under a different competence act, obtained in the course of operational activities by a non-judicial authority can often be converted to operational information and conveyed to the competent authority with the purpose of initiating operational and exploratory activities, including operational control, aimed at obtaining evidence for the purpose of future criminal proceedings.

In this respect, the appropriate action is the prosecutorial control exerted over operational and exploratory activities, having regard, in particular, to ensuring the legality and correctness of the process of initiating and conducting these activities.[4]

[1] Competence acts create a legal framework for the formation of new services. They regulate key issues concerning the organization and functioning of these services. The competence acts currently applicable to Polish government services include, inter alia, the Act of 6 April 1990 on the Police (consolidated text Journal of Laws of 2015, item 355), the Act of 12 October 1990 on the Border Guard (consolidated text Journal of Laws of 2014, item 1402), the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (consolidated text Journal of Laws of 2010, No. 29, item 154 as amended), the Act of 9 June 2006 on the Central Anticorruption Bureau (consolidated text Journal of Laws of 2012, item 621 as amended), the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service (Journal of Laws of 2006, No. 104, item 709 as amended), the Act of 16 November 2016 on the National Treasury Administration (consolidated text Journal of Laws of 2016, item 1947).

[2] Police, Border Guard, Military Police, National Treasury Administration, Internal Security Agency, Central Anticorruption Bureau.

[3] Special services: Foreign Intelligence Agency, Military Intelligence Service, Military Counterintelligence Service.

[4] Statement of reasons for the project of the Regulation of the Minister of Justice of 12 August 2016 on the manner of carrying out prosecutorial activities as part of control over operational and exploratory activities.

Systematics of counter-detection activities relating to the protection of criminal correspondence

From the theoretical point of view, counter-detection activities can be divided into tactics and techniques of criminal correspondence protection.

Tactics of correspondence protection involve the solutions and criminals' behaviors aimed at maintaining the containment of the group of interlocutors and the conversation confidentiality, preventing the identification of interlocutors, and, consequently, preventing disclosure and registering of criminal activity in the form of evidence. The following tactics can be distinguished:

1. use of anonymous telephone systems,
2. criminal slang,
3. encryption of correspondence,
4. self-control,
5. disinformation activities,
6. jamming the eavesdropping devices,
7. counter surveillance bug sweeping,

Technique of correspondence protection involves general technical measures (devices, applications), which make it difficult for law enforcement authorities to trace, control and register criminal correspondence in the form of evidence. Technical measures for the protection of correspondence involve the use of SIM boxes.

In times of the dynamic technological progress, there is a demand for the newest solutions based on the so called legal jurisdiction[5] Web servers, email accounts and instant messengers, which serve to ensure „safe" and anonymous communication in the course of criminal activity.

Anonymous phone systems

The desire to conceal the content of phone conversations compels the criminals to create anonymous telephone systems, based on far-reaching self-discipline in maintaining mutual contacts.

As regards this type of contacts, the following rules are followed:

– in order to remain impersonal and unidentified, the existing legal regulations[6] allow for purchasing SIM cards registered to other individual or entity being unrelated to the card user;
– phone conversations are conducted in a narrow circle of most trusted people (involving one or more interlocutors), the so called one-to-one phone conversations;
– phones and SIM cards must not have been previously used to conduct conversations with other interlocutors;
– phone devices must not have previously been running on other SIM cards, namely the so-called "safe" – not registered for a fabricator;
– none of the interlocutors should register a SIM card or recharge it using a different phone or a bank account;
– phones are replaced cyclically with new ones by all interlocutors;
– information about the new phone numbers is delivered in person (not by text messages sent from the previous numbers);
– previously used phones are not used to operate other SIM cards (they are usually destroyed);
– phone numbers of foreign mobile operators (Ukrainian, Slovak, etc.) are used in Poland;
– phones remain under permanent control of the holder.

In the opinion of its users, the compliance with the above rules allows obtaining a relatively hermetic and anonymous telephone system.

Criminal slang

Criminal slang is a specific language, based on the distinctiveness of the criminal underworld.[7] It differs from an official language by its lexis, phraseology and changed meaning of the vocabulary, but not grammar. It is a form of encrypting conversations, intended to conceal their actual meaning (semantic connotation). There are three levels of this type of safeguarding: low, medium and high.[8]

[5] Registration data, information associated with a particular email account and correspondence content can be made available only by order of the Court having jurisdiction over the owners of the domain (American, Russian, etc.).

[6] Anti-terrorism Law dated 10th of June 2016, (Journal of Laws 2016, item 904). Prepaid cards are to be registered personally upon proof of buyer's ID card or passport. Scanned copies, copies and xerox are not valid documents, therefore they do not enable the buyer to purchase SIM cards. Children who have ID cards can register the card individually on the provision that they are at least 13 years old. The regulations of the telecommunication law do not specify the limit in the amount of purchased pre-paid cards, however they oblige the user to register the data. The service provider is obliged to confirm the data subscribed to each MSISDN number of each SIM cars. (Information taken from: http://www.cik.uke.gov.pl/obowiazek-rejestracji-kart-prepaid-20220 [access: 19.09.2017].

[7] Common crime - e.g. frauds, beatings, robberies, trafficking of firearms, soliciting lewd conduct. Drug-related crime – e.g. manufacturing, smuggling and trading in narcotic drugs and psychotropic substances. Economic crime – e.g. smuggling and trading in excise goods, extortion, bank and tax fraud.

[8] Referring to the level of encryption, whereby the particular terms are characteristic for a given criminal environment

The phrases and expressions used are characteristic for particular criminal environments present throughout the country or in any part thereof, for example, in a given region or voivodeship. The conversations can be conducted using a more understandable subcultural (youth-criminal) slang, characterized, inter alia, by a simplified vocabulary, mental shortcuts, profanities. The analysis of correspondence related to criminal activity between the individuals maintaining frequent contacts often leads to discerning the „structure of the criminal group," , i.e. the system of links between these individuals, as well as the „hierarchy", i.e. the types of subordination and relationship between them.

The exemplary terms of a criminal slang related to trading in drugs (the so called narco-slang) are those referring to the drug type, quantity, weight and quality as well as the form of payment for the purchase. With regard to marijuana, the following terms are used: *trawa, ziele, zio*ło, *baka, maryśka, zielone, palenie*; with regard to hashish: *afgan, czekolada, hasz, gruda, lepik*; with regard to amphetamine: *amfa, białe, władek, ścierwo, bielinka*; with regard to cocaine: *koko, koks, biała dama*; with regard to ecstasy: *kółko, cukierki, tabsy, pix*; with regard to the quantity and weight: *klocek, dżis, polówka, sztuka, jedynka*[9]; with regard to the form of payment: *za hajs, w kredo*.

A separate attention is deserved by slang vocabulary associated with the processing, production and illegal trading in tobacco, which is often characterized by a low semantic connotation. The vocabulary used refers to the types, brands and quantities of these products. For example the terms: *ciemny, jasny, czarny* indicate the type of tobacco, *malwiny, marchewki* refer to the Marlboro brand, while *tona* describes one thousand cartons.

Obviously, the above mentioned slang terms do not cover all the vocabulary of this type, however, they present a mechanism of creating and using this slang.

A correct interpretation of camouflaged phone conversations made by persons subjected to operational control requires paying attention to certain constant rules (elements), also occurring as immutable, uncontrolled and natural behaviors in everyday life. One of such elements is the *principle of rational behavior*, when, for example, an order is placed or transaction scheduled (meeting arranged by phone, during which the drugs are to be purchased and money collected by the drug dealer), but the purchase/transfer is not confirmed by phone. In contrast, *rational behavior* always assumes the *principle of feedback information*, i.e. informing about being unable to attend the meeting or about cancellation of scheduled (by phone) transactions or meetings. Of course, it is important to confirm that the communication/correspondence is based solely on the controlled phone or phone number.

Another rule applying to interpersonal communication is the *principle of verbal (language) parsimony.* In the case of (permanent or *ad hoc*) criminal transactions (drug-related or other) there is no need for using the whole terms (including slang terms) describing the goods[10], prices, quantities, etc. Instead, the abbreviations are frequently used[11], whose actual meaning can be inferred from the context of the previous correspondence (conversation).

The use of a specialized criminal slang in correspondence often entails the need for a court-appointed criminal slang expert[12] to interpret material obtained as a result of the procedural eavesdropping or operational control.

Encryption of correspondence

A popular counter-detection measure is encryption of communication, which includes traditional forms of encryption, modern technical measures and specific ciphers.

Traditional encryption consists simply in using words in the context that prevents or makes it extremely difficult to understand their meaning for the person who does not hold an additional information, i.e. the so called key.

As part of counter-detection activities, criminal organizations also use modern IT and communication technologies intended for easy real time communication, such as encryption tools or secure Web sites.

A specific form of encryption is the use of very rare dialects (e.g. Uyghur, Nenets, Adyghe, Mari or Georgian).

Self-control

An example of self-control as it pertains to the protection of criminal correspondence, is a frequent exchange of prepaid mobile phone cards. In practice, it forces the law enforcement authorities to identify a new phone number, but also, in compliance with the statutory procedure, entails an obligation to

and the vocabulary used is more or less clearly indicating the type of criminal activity, e.g. drug trafficking.

[9] http://www.narkoslang.pl/slowniczek_wyrazen.html [accessed on: 24.08.2016].

[10] Objects from an offense, which are subject to forfeiture, or objects, the manufacturing and transportation of which or trading in which is prohibited, as well as the acceptance or giving of a financial advantage.

[11] For example, *to, co ostatnio; tamto,* etc.

[12] http://www.narkoslang.pl/narko_adm/uploads/files/biegly_sadowy_jacek_wrona.jpg [accessed on 24.08.2016].

impose another operational control on the new phone number. The conscious criminals are aware that the procedure of implementation of a new operational control takes time which creates a time window for „safe" criminal activities.

Another ad hoc activity consists in clearing out the memory of mobile devices when the correspondence has been completed, which prevents law enforcement authorities from acquiring the details (content) of correspondence and contact data.

Using SIM boxes

SIM boxes contain one or more SIM cards; they are also known as FCT (Fixed Cellular Terminal) devices or GSM gateways. There are several types of devices intended for telecommunication traffic transfer available on the market, including GSM adapters, GSM gateways, SIM servers. The simplest of these devices are merely the interface between the PBX and the GSM Network Termination and require the attachment of a standard GSM phone, while the most complicated devices enable the connection to the fixed network through a 2 Mbps bandwidth connection with a concurrent attachment of dozens of SIM cards.

The primary purpose of this type of devices is to provide institutional subscribers using a private telephone network (companies, offices) with a connection to the mobile network. The SIM boxes combine the functionality of the mobile and fixed network terminals, hence they can be used for transferring telecommunication traffic (re-routing calls from other telecommunication networks to the mobile network and bypassing the inter-operator point of contact between these networks). As a result of such re-routing, an established fixed-to-mobile network connection is seen by a mobile network operator as a call initiated within his own mobile network (called on-net) (Kłosowski, 2007).

The traffic that is transferred through the SIM boxes can originate from several different sources:

1. international operators re-routing the traffic from foreign fixed and mobile phone networks to Poland, including the subscribers of Polish mobile phone operators using roaming services within foreign networks;
2. national operators providing services within the national fixed network;
3. subscribers to Voice over IP services, establishing connections using the so-called soft-phones (e.g. instant messaging) or regular telephones, getting into the phone system, inter alia, by using the so-called prepaid scratch cards. It should be noted that the subscribers, whose calls are transferred, may either be aware of this fact and then consciously choose the services offered by the provider, or they can be unaware, in which case the process takes place without their operator's consent and permission (as can be seen on the above example of the subscribers using roaming services).

It should be pointed out here that the GSM boxes, when used properly for the purpose for which they were created, i.e. to connect subscribers to the GSM network, do not interfere with any activities related to the protection of security and public order. The possible identification problems appear only when such devices are used for traffic transfer, i.e. contrary to the intended purpose.

The calls routed to mobile networks through the SIM boxes have the number display function blocked by the user (CLIR- *Calling Line Identification Restriction*). As a result, there is no information about the actual number of the subscriber initiating the call. The only number displayed (true or false) is that of a SIM card that was used for routing the connection to the mobile network. Therefore, neither the mobile network operator, nor the receiving subscriber are informed about the number of the initiating subscriber or are informed incorrectly. This means that the number displayed to receiving subscriber is not in fact the actual number of the initiating subscriber, but of a SIM card inside the SIM box used to route this connection.

When the SIM box is used, the mobile network operator obtains only information about the owner of the device (SIM card number and box location). However, no information about the caller is made available. For it to be available, the owner of the SIM box would have to collect information about the traffic within his own network as well as about the assignment of the network's end devices to individual users.

The inability to determine the initiating number, and, consequently, the caller's identity, make it difficult to achieve the following objectives of forensic analysis:

1. determination of interconnections between phone numbers;
2. determination of the phone numbers contacted by the particular number within a specified time period;
3. selection of the phone numbers which were most frequently contacted by the particular number on specific days and hours;
4. drawing up a list of the most frequent connections made by the particular number;
5. determination of links between phone numbers other than direct connections;
6. positioning the phone number in relation to the transmitting antennas within a specified time period;

7. formulating conclusions about lifestyle.

The above obstacles can impede the eavesdropping or control.

Disinformation activities

Disinformation activities consist in misleading the law enforcement authorities, inferring their interest in a person or a group and testing their efficiency and the level of activity by supplying false information. Disinformation can take place in the course of an operational control or eavesdropping.

With regard to the circulation of information, disinformation takes the form of conscious omission of certain information, suggesting information by means of providing them in a particular order, resorting to lies, simulation, simplification or even fraud. By manipulating information, the criminals can achieve the following results:

– supply false information;
– supply invalid or unimportant information and omit important ones;
– supply important information as irrelevant ones;
– prepare information as a result of deliberate interventions, supply ambiguous information in order to make it more difficult to understand them;
– supply excessive information in order to cause information chaos;
– supply pseudoinformation, i.e. information delivered by different messages, but relating to the same subject;
– supply parainformation, i.e. subjective information resulting from erroneous interpretation of the message contents.[13]

Jamming the eavesdropping devices

The eavesdropping devices are jammed by using the equipment generating radio noise on the same frequency and with the same modulation as the original wave. Such equipment can interfere with eavesdropping devices.

Other equipment used can distort recorded sounds, which renders them incomprehensible and unusable.

Anti-surveillance screening

Anti-surveillance screening consists in checking the premises for the presence of external optical systems (camcorders, cameras, etc.), active or inactive electronic components (transmitters, recorders, etc.), emission of IR signals (Infra-red transmitters), emission of radio signals in the range of up to 25 GHz, emission of radio signals in the low frequency range (below 1 MHz), emission of identified radio signals in the frequency of up to 3 GHz, emission of subcarrier frequencies in the phone network and 220 V.

Role of counter-detection activities in criminal activity

Counter-detection measures are applied as a reaction to detection activities carried out by law enforcement authorities, such as the eavesdropping or operational control. They have a defensive character, i.e. serve to strengthen the criminal organization in order to avoid its neutralization. The following factors determine the effectiveness of counter-detection activities:

1. appropriate technical equipment (scanners, encrypting applications);
2. situation as regards criminal activity - a one-time application of the same counter-detection measure or multiple applications of a combination of measures may be required;
3. experience and training of criminals in implementing specific activities;
4. time of reaching objective (the longer criminal activity, the higher risk of detection);
5. financial capabilities of criminal organization.

In order to avoid counter-detection activities of government authorities who, in the course of operational activities, have acquired ex-ante information about the crime being planned, e.g. scheduled (agreed) drug transactions, the criminals apply various counter-detection measures, such as:

– meetings with drug suppliers/recipients are organized in places difficult to prepare an ambush intended to catch the criminals in the act of committing a crime (previously verified places, open spaces, hardly-accessible, private areas).
– meetings are organized in places suitable for carrying out counter-observation by criminal accomplices;
– if the meeting venue needs to be changed at the last minute, information is passed by using other means of correspondence.

The role of counter-detection activities is to reduce the effectiveness of law enforcement authorities in collecting operational information and to interfere with transforming operational material into admissible evidence.

In addition, these measures are meant to prevent identification and tracking of criminal activity and to interfere with collecting and securing evidence (e.g. generated by tapping the phone) or discerning the structure of a criminal organization.

Summary

Counter-detection measures are an indispensable element of any criminal activity, playing a role of

[13] http://www.ktime.up.krakow.pl/symp2011/referaty2011/babik.pdf [accessed on 25.08.2016].

the „safety pillar" and guaranteeing impunity for committing criminal acts. In the opinion of the criminals, applying far-reaching measures of precaution, e.g. self-control, guarantees business security. As regards criminal activity, the greatest achievement is to ensure total anonymity and conceal the criminal acts. Criminal behavior described herein can be referred to as counter-detection techniques and tactics. The understanding and proper diagnosing of these activities by law enforcement authorities allows for the selection of an appropriate detection techniques/ tactics, both at the operational and procedural level.

Bibliography

1. Bożek, M. (2015). Charakterystyka ustawowych *uprawnień operacyjnych służb specjalnych*, *Rocznik Administracji Publicznej, 1*.
2. Babik, W. (2011). O manipulowaniu informacją w prywatnej i publicznej przestrzeni informacyjnej, http://www.ktime.up.krakow.pl/symp2011/referaty2011/babik.pdf [accessed on 25.08.2016].
3. Dolecka, A., Łodziana, T. (2015). Taktyczne aspekty stosowania kontroli operacyjnej. In: E.W. Pływaczewski, W. Filipkowski, Z. Rau, (red.), *Przestępczość w XXI wieku – zapobieganie* i zwalczanie. Warszawa: Wolters Kluwer Polska.
4. Drajewicz, D. (2011). Gloss to the decision of the Supreme Court of 25 March 2010, file no. I KZP 2/10, *Prokuratura i Prawo, 9*.
5. Herzog, A. (2007). Wykorzystanie materiałów operacyjnych w postępowaniu dyscyplinarnym prokuratorów, *Prokuratura i Prawo*, *2.*
6. http://www.narkoslang.pl [accessed on 25.08.2016].
7. Kaczorkiewicz, D. (2014). Granice inwigilacji społeczeństwa w zakresie czynności operacyjno-rozpoznawczych. In: E. Cała-Wacinkiewicz, K. Flaga-Gieruszyńska, D. Wacinkiewicz, (ed.), *Obywatel – państwo – społeczność międzynarodowa*. Warszawa: C.H. Beck.
8. Kłosowski, A. (2007). Opinia specjalistyczna w zakresie wpływu transferu ruchu z pominięciem punktów styku sieci telekomunikacyjnych (za pomocą urządzeń FCT) na realizację przez operatorów telekomunikacyjnych zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Warszawa.
9. Mąka, J. (2011). Kontrola operacyjna i podsłuch – ocena na tle praktycznego stosowania, *Przegląd Bezpieczeństwa Wewnętrznego, 4*/11.
10. Skorupka, J. (2011). Krytycznie o stanowisku Sądu Najwyższego w kwestii legalności kontroli rozmów telefonicznych, *Prokuratura i Prawo*, *4*.
11. Act of 24 August 2001 on the Military Police and Military Law Enforcement Units, Journal of Laws of 2001, No. 123, item 1353.
12. Act of 6 June 1997 . The Penal Code, consolidated text Journal of Laws of 2016, item 1749).
13. Act of 6 June 1997 . The Penal Code, consolidated text Journal of Laws of 1997, No. 89, item 555 (as amended).

Translation Rafał Wierzchosławski