Paweł Łabuz, Ph.D.
Lecturer at the 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 organizations aimed at reducing the effectiveness of surveillance conducted as part of operational activities

Summary

The article presents the essential aspects of tactics and techniques applied by criminals with an aim to reduce the effectiveness of surveillance conducted as part of operational activities. The possible actions adopted by criminals with the purpose of preventing surveilling authorities from detecting their activities are 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. This article points out the advantage of having comprehensive knowledge of criminal tactics and techniques used in this field.

Keywords: surveillance, counter-detection activities, criminal tactics

Introduction

Counter-detection activities as they pertain to surveillance conducted as part of operational and exploratory activities include any operations undertaken by offenders, aimed at preventing surveilling authorities from detecting their activities and successfully fulfilling the goals set forth.

Nowadays, the above activities include a wide spectrum of forms, methods and measures (mainly technical), 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 target[1].

Criminals have for a long time recognized the benefits stemming from applying counter-surveillance measures, and as such they use various forms and methods, including specialist techniques and advanced technologies.

The surveillance of individuals, places and objects undertaken by state services[2] may represent their fundamental operational and exploratory activity, for example in case of intelligence and counter-intelligence services that gather information solely for operational and analytical purposes, unlike the police, whose main task is to prevent and detect offenses as well as identify the perpetrators. It should be pointed out that there are many surveillance methods differing in the degree of interference, ways of registration and analysis as well as the duration. The surveillance can be either overt or covert.

In general terms, the surveillance pertains to people, assets, areas of strategic importance to companies, military and government. Despite being used on a large scale, preventively, repeatedly and

[1] Person placed under surveillance by authorized services. Person of interest to (invigilated by) state services as part of the conducted operational and exploratory activities.

[2] State service – police or special service. Pursuant to Art. 11 of the Internal Security Agency and Foreign Intelligence Agency Act, special services include the Internal Security Agency, Foreign Intelligence Agency, Military Counterintelligence Service, Military Intelligence Service and Central Anticorruption Bureau. It should be pointed out that the above regulation does not define the term "special service". All the remaining authorities, services and institutions are referred to as "police".

without the subjects' knowledge, the surveillance, in accordance with its definition, is carried out discreetly. Another type of surveillance is the so called "overt surveillance", when the subject is informed about the monitoring being installed regardless of its forms, e.g. monitoring of computer hardware or facilities by industrial cameras (Podsiadły, 2007).

Systematics of police surveillance

Police surveillance[3] is an operational and exploratory method directed at achieving certain objectives, such as:

- gathering certain information or confirming information previously obtained from different sources about persons, objects or places;
- verifying or confirming the presence of certain persons in a given place;
- determining membership of criminal organizations (Gołębiewski, 2008);
- determining personal contacts and physical contact points (hideouts, illegal storage facilities, etc.);
- assisting in setting up ambushes with the purpose of apprehending perpetrator(s) in the commission of the offense.

The catalog of objectives serves as an orderly system for acquiring information and should not be treated as complete. Certain objectives may appear before or during the surveillance process. It is not possible to precisely determine the plan (scenario) and difficulty level of the activities, camouflage used by the surveilling authority in order to maintain a conspiracy as well as the behavior of a target and his collaborators and the counter-detection measures used.

Observation (herein referred to as surveillance) is a common activity (behavior), indispensable for recognition of the surrounding reality. It makes it possible to observe various phennomena in an undisturbed natural environment. Surveillance can be carried out using the observer's senses or by reinforcing them with technical devices (binoculars, microscope, camcorder) or more sophisticated devices based on modern technology (electronics-interface). Another form of surveillance is the Global Positioning System (GPS), which is becoming increasingly available in vehicles, cellular phones and other mobile devices (Kosmaty, Kudła 2012).

[3] Surveillance concerns such individuals, places, objects and means of transportation in relation to which state services and other authorized entities have legal grounds to initiate certain actions (according to the Parliament bill on operational and exploratory activities).

Many cities in both Poland and Europe[4] have well-functioning city monitoring systems, whose only objective is broadly understood improvement of security, achieved by eliminating the need for constant surveillance and automatic detection of emergency situations. Certainly, the CCTV infrastructure should meet certain requirements, in particular:

- detecting fires,
- performing multidimensional analysis of the behaviour of groups of people,
- recognizing the way of moving of individuals,
- recognizing facial expressions,
- recognizing vehicle license plates,
- identifying objects that may endanger public security (http://monitoring24alarmy.blogspot.com/2014/12/monitoring-miejski-i-jego-wpyw-na.html).

Nine state institutions authorized to conduct surveillance include the Police[5], Border Guard, Central Anticorruption Bureau, Internal Security Agency[6], Military Counterintelligence Service, Military Police, National Treasury Administration, Foreign Intelligence Agency and Military Intelligence Agency. As of 1 Febuary 2018, the Act on the State protection Service came into force, which gives teh right to conduct surveillance activities for the officers SPS – art. 21 item 8.

Surveillance allows collecting information about criminal activity prior to the initiation, during, or after completion of a criminal proceeding.

Systematics of special services' surveillance

Surveillance conducted by special services, e.g. intelligence services has different purposes as compared with the police, which results from a different scope of competences. It does not

[4] It is estimated that the average Londoner gets recorded approx. 300 times a day. In Great Britain there are more than four million cameras.

[5] Art. 15, section 1, item 5a. Police officers shall, in the course of their activities, be entitled to conduct surveillance and, by using technical means, to record video of the scenes of the events occurring in public places and, in the case of operational and exploratory or administrative and order maintenance activities undertaken pursuant to the Act, to record audio accompanying the events. Act of 6 April 1990 on the Police. Journal of Laws of 2017, item 60. Consolidated text.

[6] Art. 23. 1, item 6. Officers of ABW shall, in the course of their activities, be entitled to conduct surveillance and, by using technical means, to record video of the scenes of the events occurring in public places and, in the case of operational and exploratory activities undertaken pursuant to the Act, to record audio accompanying the events. Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency. Journal of Laws of 2017, item 60. Consolidated text.

necessarily lead to the apprehension of a perpetrator in the act of committing a crime, especially when the information collected can be used to set further operational objectives (e.g. recruiting the target or persons in his milieu), or to test the mobility and effectiveness of foreign counterintelligence services[7].

The scope of technical methods used is very extensive and complex, due to an indefinite duration of the surveillance, which aims at collecting as much information as possible about the target's lifestyle, contacts, habits and other behaviours that are relevant to intelligence services (civilian or military). The target does not necessarily have to engage in criminal activity, but he may be proficient in gaining access to information that are not publicly available (secret).

It can be stated that the surveillance supports special services in gathering information about the target's timetable, contact addresses, established contacts, mental condition, daily routine, etc. When conducted properly, the surveillance allows to determine whether the target is skilled in using operational techniques, e.g. counter-surveillance or escaping surveillance whenever convenient. Depending on the level of knowledge about the target, the surveillance objectives can be general or very precisely formulated. General objectives include revealing the target's timetable or verifying his contact addresses. Detailed objectives include determining the time and place of the meeting and documenting this event (Schemat ułatwiający…, 2013).

In the case of counterintelligence services, the main objective is to verify espionage activity of the target of broadly understood operational interest.

Counter-espionage is one of the main tasks of counterintelligence services and it involves recognizing certain events as well as activities of foreign agencies – a long term process entailing the use of wide selection of operational methods such as the surveillance, which makes it possible to find out more about personal contacts, contact points, vehicles and ICT-based communication channels used by the potential spy as well as his personal information. The use of other operational methods can, in turn, verify the initial information (suspicion) about foreign intelligence activity and facilitate the implementation of adequate counter-espionage measures (Łabuz, 2017).

Persons placed under surveillance by special services can be quite challenging as they may represent specially trained foreign intelligence officers or agents (spies) with long service record, who are accustomed to using counterintelligence measures in order to evade surveillance or direct it onto a favorable path. It is generally assumed that a failure to detect the surveillance gives an indication of the agent's ineptitude or reflects the fact that it was effective and camouflaged in a manner that made it impossible to discover.

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

One of the ways of converting operational information into evidence is to hear police officers who conduct surveillance as witnesses. In order to avoid exposing officers or the nature of operational activity (covert surveillance), it is possible to make use of the institution of incognito (anonymous) witness[8]. Such procedure facilitates the use of evidence obtained in the course of operational and exploratory activities such as covert surveillance in criminal proceedings.

As it is known, extrajudicial information often provides more reliable and accurate knowledge, both about the event and its circumstances in relation to the witness or the suspect (including the knowledge that cannot be used or verified in the course of the proceedings, even though it may be accurate with regard to certain essential elements of the event) (Stryszowski, 2015).

Hence, information gathered during the surveillance can, in certain specific circumstances, constitute a basis for initiating a criminal proceeding or be relevant for the proceeding pending. In practice, once available and declassified, 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.

Systematics of counter-detection activities

From a practical point of view, the following tactical measures taken by the offenders can be distinguished:

- self-control,
- counter-surveillance,
- masking (disguising),
- reconnaissance,

[7] The term "foreign services" means any intelligence services or counterintelligence services other than domestic.

[8] Art. 184 § 1 of the Code for Criminal Procedure. If there is a justified fear of danger to life, health, liberty or property of significant size of the witness or the person next to him, the court, and in preparatory proceedings the prosecutor may issue a decision to keep secret the circumstances allowing disclosure of the identity of a witness, including personal data if they are not relevant to the outcome of the case. Proceedings in this regard takes place without the participation of theparties and is subject to state secrecy. The decision ignores the circumstances referred to in thefirst sentence. Act of 6 June 1997. *The Penal Code*. Journal of Laws of 2016, item 1243. Consolidated text.

– disinformation activities,
– escaping and directing surveillance.

A proper *self-control* aims at preventing the surveilling authority from making observations, i.e. obtaining relevant information. An example of self-control applied in the course of criminal activities is verification of the place designated for a drug transaction in terms of the presence of monitoring or bystanders (potential witnesses, etc.), performed by a target who suspects that covert surveillance may have been set up.

Such places can include the premises that are unavailable for unauthorized persons, e.g. private residences[9], non-residential premises (business premises, shops, corporate offices, etc.), other premises (garages, warehouses, cellars, gazebos, etc.), fenced areas (fenced plots, allotments, etc.). Unauthorized or forced entry into such premises is referred to as "intrusion upon seclusion" and it constitutes an offence[10]. There are also certain public places that are less amenable to conducting the surveillance, e.g. the places of assembly of informal sub-cultural groups (e.g. football hooligans), homosexuals, religious sects, nationalist groups, etc.

The effectiveness of counter-surveillance also depends on other factors such as certain circumstances and the duration. For example, the surveillance conducted at night, in the early morning or at dusk can be challenging, due to limited visibility. Other factors include lower pedestrian traffic, lower number of clients at the points of sale, season of the year, mass events (rallies, assemblies, sporting events, etc.).

The above factors are permanent element of self-control techniques used by the targets, who frequently choose the sites that either interfere with or completely prevent the surveillance, thus rendering it ineffective and leading to the exposure.

Reconnaissance is used by criminals to determine whether the particular person is under surveillance or whether certain behavior will result in placing a person under surveillance (arouse interest). Occasionally, reconnaissance can be equated with self-control or criminal provocation (test, experiment).

In practice, reconnaissance involves:
– video monitoring – an analysis of video recordings allows the identification of individuals who stay in certain areas for too long and for no logical reason, e.g. loitering around the doors, garage, vehicle, telephone junction box;
– video recording and analysis of the surroundings of a person suspecting that he/she may be under surveillance – using the simplest video recorders (wearable, placed inside clothes).

Owing to their awareness as well as counter-surveillance measures used, criminals are capable of gathering various information, e.g. concerning the potential victims of crime and the site where the criminal transaction will be concluded with special emphasis on possible distribution of observation points, and the possible forms of surveillance, including masking measures and cover stories, that could be used by the surveilling authority. The site inspection performed in the capacity of a would-be target, allows criminals to choose the time, place and circumstances that prevent surveillance.

Counter-surveillance aims at determining whether the surveillance was set up by competitive criminal organization or law enforcement authorities. It allows the identification of both mobile and permanent observation points. Counter-surveillance is also used by the targets (criminal groups) who assume that they may be subject to surveillance or those forced to relocate while under surveillance.

The prefix *counter-* refers to the situation where the targets and law enforcement authorities observe each other. The professional law enforcement surveillance teams have internal units responsible for detecting criminal counter-surveillance. In turn, criminal counter-surveillance aims at detecting and identifying the observers (observation points, vehicles used, technical devices, etc.), determining their activities, movement patterns, forms of communication or any other relevant information that will help the targets to adapt to the situation and learn the methods of surveillance (for the future) used by a particular state service.

Masking, i.e., *masking activities of the police* are meant to create or exploit misperception of third parties about the real meaning of the events, purposes of objects or identity of persons subject to police actions. In the case of criminal activity, masking[11] consists in creating situations (behaviors) that appear natural and insignificant, in order to convince the observer that it is pointless to record (document) them, as they do not fulfill the objectives of the surveillance. Such

[9] In private dwellings, surveillance can be used only as one of the forms of operational control, i.e. "obtaining and recording video and audio of people inside the premises, means of transportations or in non-public places".

[10] Art. 193 of the Penal Code. Whoever breaks into someone else's house, apartment, premises, quarters, or a fenced plot of land, or despite a demand from an authorized person does not leave such a place shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year. Act of 6 June 1997. *The Penal Code*. Journal of Laws of 2016, item 1137. Consolidated text.

[11] According to the dictionary of Polish language; make something or someone invisible, conceal one's own true intentions, feelings, character.

actions require a high level of professionalism and often also creativity to be shown in the process of masking. An example of masking activities can be a transaction during which a significant information or item is to be transferred to a person, while the task of the surveillance team is to identify this person (target's contact), the manner of transferring and the item to be transferred (object, record, etc.). Similar situations can frequently occur in different configurations. Even though the above situation may not appear to be of value to the surveillance team, it should definitely be documented. For example, when receiving a treat or lighting a cigarette, the target could transmit an oral information or an item concealed in the cigarette pack or the lighter to his contact in an invisible manner.

Therefore, it is a common practice to record and document all behaviors and contacts of the surveilled target. The analysis of the complete recording (report on the activities) provides important information, for example about the target's contacts (as one of the objectives of surveillance), or about other behaviors, such as using counter-surveillance elements in everyday life. In the case of a dynamic surveillance, aimed at apprehending the target at the time of the illegal transaction, i.e. in the act of committing a crime, certain information (e.g. relating to personal contacts) or behaviors can be skilfully masked by the target. In such a situation, the decision on apprehending the subject is to be made by the leader of the surveillance team, who maintains direct contact with the party requesting surveillance[12]. The system of masking counter-surveillnance activities is in many ascpects equated with disinformation activities.

Disinformation activities consist in misleading law enforcement authorities by targeted transmission of false information. Disinformation can be applied by the target, who, after becoming aware that he was under surveillance, has precisely identified his observers, while the latter, still unaware of their exposure and having confidence in their camouflage measures, are continuing the surveillance. Such a situation can result in obtaining useless and false surveillance material (information).

The above is in line with the fact that in the Polish language dictionary, disinformation is defined as false, mendacious or unverified information, which does not improve the recipient's knowledge. Etymologically, the prefix *dez-*, when used in Polish compound words (especially before a vowel), means the opposite (organizacja [organization] – dezorganizacja [disorganization]), (orientacja [orientation] – dezorientacja [disorientation]) or even the lack of acceptance, consent (aprobata [approval] – dezaprobata [disapproval]). Hence, disinformation consists in providing false information meant to mislead the recipient. It should be assumed that the provision of false information is usually deliberate, meant to achieve certain benefits from the lack of knowledge of a misinformed person or institution. However, it cannot be excluded that disinformation will take place unintentionally as a result of misunderstanding or distorting source information (Wrzosek, 2005).

Escaping and *directing surveillance* results in breaking contact with the observer. The target takes the observer by surprise, diverting his attention or dulling his vigilance. An example of surprising behavior can be red light running, avoiding traffic congestion by driving along the pavement between pedestrians, and many other unpredictable behaviors constituting an offence.

Other forms of escaping surveillance include switching from walking to riding a sportbike (as a passenger), bicycle, skateboard, informing the police (by phone or personally) about the "suspicious" individuals (observers) allegedly following the target, who expresses concern about his life and well-being, or informing about vehicles parked for a long time in the local parking lot. When reported to the duty police officer, such situations naturally trigger police intervention in response to the citizen report., i.e. performing ID checks on the suspicious individuals or inspecting the vehicle.

Another element of criminal tactics is directing (leading) the surveillance team by a target who is aware that he is being followed. With this knowledge, the target stays within sight of the observers and does not interfere with the surveillance, but refrains from any activities that could be informative, e.g. leading the observers to identify the target's unknown contacts, addresses visited, etc.

Legalization of criminal activities by state service officers on the example of police surveillance

Counter-surveillance is also used by state service officers who carry out operational and exploratory activities and, at the same time, engage in criminal activity, either individually or in cooperation with other officers or common criminals. The above constitutes an exceptionally difficult situation in terms of crime detection and collection of evidence, because the officers-criminals have a statutory right to use a whole range of legal tools, including operational methods.

Therefore, the above situation carries a significant risk of exposure for officers who investigate criminal activity of such individuals. Additionally, officers-criminals, having access to police and non-police

[12] For example: requesting party – organizational unit of the police requesting the surveillance from the technical and operational support unit.

databases, can, under the guise of routine checks, verify whether their accomplices in a criminal activity have been placed under surveillance. It has been demonstrated that officers engaging in criminal activity often think of themselves as being under the umbrella (untouchable), depending on the position occupied within the police unit and the type of unit they serve in. For example, officers of the units that have administrative supervision over all operational and exploratory activities within a given area, have full knowledge of the criminal underworld in this area.

When such individuals are placed under surveillance, it can be conducted by a different service or by units competent for internal affairs[13], ideally without jurisdiction over a given area (voivodeship, garrison, command, branch office, directorate, etc.). Such a practice is intended to eliminate the risk of exposing the observer or disclosing the activities scheduled.

Physical surveillance of an officer-criminal requires moderate use of commonly known methods of observation, other than standard methods of masking and cover stories, as well as an ongoing monitoring of counter-detection measures potentially implemented by the individual under surveillance that would confirm his awareness of operational activities he had been covered with. The systematics and scope of the surveillance is easier to determine as it covers certain permanent places of residence and personal contacts, involving place of work (police station), contacts (colleagues, including police officers), place of permanent residence, vehicles, public transport as well as other permanent places and objects known to the surveillance team.

Police surveillance may also be initiated by officers-criminals as a counter-detection measure, under the guise of own operational activity, whereby certain false information may be fabricated. The objective of criminal surveillance may be to disclose the witnesses or personal sources of information providing information on criminal activity to other services or internal affairs units. In addition, it can aim at identifying new areas to be covered by criminal activity, for example, new drug dealers distributing narcotic or psychotropic substances on their own, or the competition in a given crime area.

Active duty police officers engaging in criminal activities and, simultaneously, carrying out their police duties try to work closely together with all police, internal affairs and control units having jurisdiction over the particular area in order to achieve police coordination within this area and be able to transmit information (disinformation) with the purpose of verifying the interest in a given place or person. They may also try to collect information about the police subject of interest through informal social contacts.

Role of counter-detection activities in criminal activity

The use of counter-detection measures discussed above is a form of a defence mechanism that facilitates avoiding criminal liability in face of operational activities, i.e. the surveillance carried out by law enforcement authorities The following factors determine the effectiveness of counter-detection activities:

1. appropriate technical equipment (scanners, jamming devices);
2. operational situation in relation to criminal activity – a one-time application of a single 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 needed to reach the objective (the longer criminal activity, the higher risk of detection);
5. financial capabilities of the criminal organization;
6. cooperation (corrupt) between criminals and officers who have access to particular information (e.g. concerning subjects of police interest, actions scheduled, operations, etc.).

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

Crime is not something permanent, with immutable characteristics, causes and consequences. Its most important features are dynamism, variability and adaptation to the existing circumstances and socio-economic or political situation (Mądrzejowski, Śnieżko, Majewski 2017).

Criminal tactics entail the entire methodology of behaviours, reconnaissance, criminal intelligence, setting up hideouts and storage facilities, building cover stories, masking, covering up traces, using different forms of provocation and achieving criminal goals. The above tactical-criminal activities are part of the evolving process of criminal self-improvement.

Frequently, counter-detection activities carried out in response to police surveillance are part of a comprehensive system of criminal tactics – without doubt a poorly recognized subject by both state service and law enforcement officers, as well as scientific communities in the field of law and security science.

[13] With regard to police officers: Internal Security Agency, Central Anticorruption Bureau or Office of Internal Affairs of the Polish National Police Headquarters.

Bibliography

1. (2013) Schemat ułatwiający prowadzenie działań obserwacyjnych. *e-Terroryzm.pl, 6*(18).
2. Act of 6 April 1990 of Police. Journal of Laws of 2017, item 60. Consolidated text.
3. Act of 6 June 1997. *The Penal Code.* Journal of Laws of 2016, Consolidated text.
4. Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency. Journal of Laws of 2017, item 60. Consolidated text.
5. Dunaj, B., (ed.). (2017). *Słownik języka polskiego*. Warszawa: Wydawnictwo Wiedza Powszechna.
6. Gołębiewski, J. (2008). *Praca operacyjna w zwalczaniu przestępczości zorganizowanej*. Warsaw: Academic and Professional Publishers.
7. http://monitoring24alarmy.blogspot.com/2014/12/monitoring-miejski-i-jego-wpyw-na.html [acessed on: 4.04.2017].
8. Kosmaty, P., Kudła, J. (2012). Obserwacja – wybrane aspekty procesowe i kryminalistyczne. *Quarterly of the Management Board „Policja", 1*.
9. Mądrzejowski, W., Śnieżko, S., Majewski, P. (2017). *Zwalczanie przestępczości – wybrane metody i narzędzia.* Warsaw: Editions Spotkania.
10. Niemczyk, Z. (2013). Czynności operacyjno-rozpoznawcze i możliwość wykorzystania ich rezultatów w postępowaniu karnym. *Quarterly of the National School of Judiciary and Public Prosecution*, *3*(9).
11. Podsiadły, R. (2007). Okiem wielkiego brata – inwigilacja pracowników w firmie. *Hakin9*, *5.*
12. Stryszowski, P. (2015). Świadek incognito – algorytm postępowania. *Prokuratura i Prawo*, *12.*
13. Wrzosek, M. (2005). *Dezinformacja jako komponent operacji informacyjnych.* Warsaw: Akademia Obrony Narodowej.

Translation Rafał Wierzchosławski