UDC: 327.84:323.285(100)
DOI: https://doi.org/10.5937/pnb25- 46899
Review article

The Policy of National Security
Year XIV, vol. 25
No. 2/2023.
pp. 157-181

Milovan Trbojević[*]
Faculty of Security Studies, Educons University, Sremska Kamenica

Branislav Svirčević[*]
Faculty of Security Studies, Educons University, Sremska Kamenica

METHODS OF INTELLIGENCE SERVICES IN THE FIGHT AGAINST TERRORISM

Resume

Adequate analysis of the struggle of intelligence services against terrorist organizations requires an approach based on the methods and means of action of intelligence institutions. Terrorism is among the most represented security threats in the media and in public discourse. The increasing brutality of terrorist groups and organizations, the frequent mention in the public and the virality of terrorist acts on social networks have led to the creation of a specific fear of terrorism, which is why early detection and stopping of terrorist activities is extremely important. In the field of preventive action against terrorism, intelligence institutions play the most important role. Intelligence institutions primarily use specific methods and techniques for collecting data on terrorist threats, which enables their detection and interception. In addition, intelligence institutions also use non-intelligence methods of combat that require special analysis. On the other hand, terrorist organizations, in addition to carrying out terrorist acts, also carry out activities aimed at disrupting and disavowing intelligence institutions, which further complicates the fight against terrorism.

[*] Contact: trbojevicmilovan1@gmail.com

[*] Contact: svircevic1995@gmail.com

Key words: intelligence agency, intelligence methods, non-intelligence methods, terrorism, terrorist organization, terrorist act.

INTRODUCTION

The existence of security-threatening phenomena, including terrorism, requires a systemic and institutional response from the state in terms of the formation of organizations or organizational units or groups within the institution whose mission is to fight against them. Taking into account that all security-threatening phenomena are multidimensional, and that the state opposes them on several levels, it is necessary to apply the principle of division of labour in the creation of institutions that oppose threats in different phases and in different forms. According to the division of activities in the fight against threatening phenomena, the role of intelligence agencies is realized most often on a preventive level, while the repressive engagements of intelligence institutions are restrictive. In terms of preventive action, we can say that the effectiveness of intelligence agencies is particularly important in the fight against terrorism, both because of the harmful consequences of this threatening phenomenon, and because of the effect of panic and fear that they produce. The importance of preventive action is also reflected in the fact that terrorist activities are directed most often against the state government, which is categorized as the greatest threat to the achievement of the goals and intentions of terrorist organizations.

The primary role of intelligence agencies as bearers of intelligence power is the collection of intelligence data on terrorist activities. Intelligence data can be collected from different sources and by means of different methods and techniques. However, sometimes the collection of data is not enough to neutralize terrorist organizations and groups, and intelligence agencies also resort to various non-intelligence methods. The decision on which method to use is made by the heads of intelligence institutions, and in certain situations where the degree of danger is increased and where urgent engagements are required, the decision can also be made by the holders of executive power. The decision mostly depends on the current circumstances and factors, as well as on which method can be used most effectively to prevent the actions of terrorist groups. The fight against terrorism in the action of intelligence agencies and other elements of the national security system requires compliance with all positive legal regulations and political-declarative acts, which prevents the abuse of the coercive apparatus.

THE CONCEPT OF TERRORISM

The etymological angle of observation leads us to look for the root of the word terrorism in the term terror, which originates from the Indo-European word *ter ortre*, which in translation means great fear, horror, etc. (Simeunović 2009, 86). Although of Latin origin, the word "terror" entered the political and scientific vocabulary through the French language, where it was used for the first time to denote the extraordinary measures introduced and applied by the Jacobins for the defence of the revolution. According to this explanation, "if the stronghold of the people's government in peace is virtue, the stronghold of the people's government in the revolution is both virtue and terror" (Dimitrijević 2002, 16).

Just because the root of the word terrorism has been determined, it does not mean that there is a general consensus about its origin. The forerunner of modern terrorism is linked to the second half of the 19th century and to the anarchist movement "People's Will" which was founded on the territory of Imperial Russia. This antimonastic organization had all the key elements of contemporary terrorist groups, and the main (historical) goal was the overthrow of the then government. Although they did not find support among the people, they carried out numerous terrorist acts, including the assassination of Emperor Alexander II in May 1881 (Miletić 2019, 5).

Each terrorist organization and each terrorist action, especially in terms of different historical circumstances and eras, has its own specificities, but there are also characteristics of terrorism that are universal and valid in all historical and social contexts and in the case of any terrorist activism, namely: use of force or violence; political character; causing fear or terror; threat; psychological effect and reaction; different victims and wider targets of attacks; targeted, planned and organized action; existence of methods, strategies and tactics of fighting; extreme violation of accepted rules; absence of humanitarian segments; blackmail, coercion and inducing obedience; desire for publicity; arbitrariness, impersonality, randomness and lack of discrimination; intimidation; emphasis on the impotence of the state; the perpetrator is an individual, group, movement or organization; symbolic nature, showing others; the unpredictability and unexpectedness of the appearance of violence;

secrecy, concealment; repetition of a series or campaign of violence; criminal, criminal character; claims against third parties (Weinberg, Pedahzur, and Hirsch-Hoefler 2004, 781).

As for the definition of terrorism, it must include all the most important elements, and not only those that seem the most attractive in the populist sense. According to the above, as a multidimensional political phenomenon, modern terrorism can theoretically be defined in the most general terms as: a complex form of organized group, and less often individual and institutional political violence, marked not only by terrifying brachial physical and psychological, but also by sophisticated-technological methods of political struggle that are usually used in times of political and economic crises, and rarely in conditions of achieved economic and political stability of a societies, systematically try to achieve great goals in a morbidly spectacular way, and inappropriately given the conditions, above all the social situation and historical possibilities of those who exercise it as a political strategy. The socially threatening opus of terrorism includes the threat of force as part of intense psychological-propaganda activity, misuse of the Internet for terrorist purposes, kidnappings, blackmail, psychological abuse, assassinations, sabotage, diversions, suicide attacks, individual and mass political murders, and the intention of manifesting less often than actual and potential political opponents, and more often on representatives of the system and innocent victims. As a form of individual, illegitimate, illegal and non-institutional violence, terrorism is always directed against certain institutions of a society, that is, against a government (Simeunović 2009, 80).

Therefore, terrorism has exclusively political interests and is aimed exclusively at the authorities, and in the event that the goals of terrorist activity lose their political dimension, it would cease to exist as a form of threat to national security. Regardless of what form and type it is, terrorism always propagates certain value categories and necessarily contains an extreme ideological-political dimension, which has exclusive views on certain ideas, processes and phenomena, which it seeks to oppose. An important feature of terrorism is the selection of the most effective method, which can achieve the greatest possible effects with the investment of minimal funds (Gaćinović 2016, 49-50).

Terrorism can be scientifically defined in different ways. Viewed from the perspective of security sciences, terrorism is a non-military and unconventional form of endangering national security. From the point of view of political science, terrorism represents a complex form of political violence directed against the government, while from the point of view of legal science, terrorism is defined as a criminal offense.[1]

As a complex political and (anti)social phenomenon, terrorism is classified according to different criteria. All classifications of terrorism have a primarily theoretical and methodological character and are not mutually exclusive. According to the role of the state, terrorism can be divided into: international (groups and individuals that are under the control of a sovereign state), transnational (groups and individuals that are not under the control of sovereign states – although they may have some support from states that approve their goals), domestic (includes only citizens of a certain country and autonomous non-state subjects) and state terrorism (its bearer is the state within its borders) (Živaljević and Jugović 2014, 8). According to the target-program orientation, terrorism can be divided into: 1. Ideologically motivated terrorism (leftist and rightist), 2. Ethno-separatist terrorism, 3. Religiously based terrorism (terrorism of sects and terrorism based on the interpretation of major religions). According to the means used by terrorists, terrorism can be divided into: 1. Classical (conventional) terrorism, 2 Biochemical terrorism, 3. Nuclear terrorism. Then, according to the methods of action, terrorism can be divided into: 1. Classic (conventional) terrorism, 2. Suicide terrorism, 3. Cyber-terrorism, 4. Narco-terrorism. The classification of terrorists according to the type of actor, shows us that the perpetrators of a terrorist act can be: 1. individuals – individual terrorism, 2. groups and organizations – terrorism by organizations and illegal groups, 3. states and national institutions – institutional terrorism (Simeunović 2009, 83- 85).

The most prevalent type of terrorism is Islamist terrorism, as a subtype of religious-based terrorism, while eco-terrorism, right-wing terrorism (in terms of ideology) and individual terrorism (in terms of the carrier) are on the rise. Islamist terrorism is the most dynamic subtype of terrorism. Extreme Islamism has given birth to a threat in the form of "lone wolves", that is, radical Islamists born or permanently settled in mostly non-Muslim countries, who, in the desire to contribute to the struggle for the embodiment of the idea of a global Caliphate, undertake individual actions, without including any other actor, thus plans for remain

[1] In the Criminal Code of the Republic of Serbia, terrorism and acts related to terrorism belong to the group of crimes against humanity and goods protected by international law. (Criminal Code of the Republic of Serbia 2017, Article 391)

uncompromised by future activities, and the chances of committing a terrorist act are greater. The recruitment of lone wolves is part of global Islamic recruitment internationalism, which, in addition to bringing fighters from all over the world to the war zone, invites all Islamist radicals to contribute to the achievement of a concrete historical goal in their countries. Also, Islamist terrorism managed to manifest itself in the form of a "quasi-state" (Islamic State of Iraq and Syria), where the terrorist organization had control over a certain territory and where it had its own military and intelligence-security forces.

The structure of terrorist organizations consists of management bodies (higher and lower) and branches or units (basic, most numerous units). It is chained with clearly defined relationships between higher and lower parts of the organization. In the highest management body of the terrorist organization, there is also a person who coordinates the "intelligence and security work" of the members of the organization. He is usually some kind of advisor to the leader of a terrorist organization. He is often assigned a team or group of "pseudo-analysts" who process the collected information, plan and program the execution of terrorist actions. The structure and extent of development of intelligence and security components depend on the type and structure of terrorist groups: in the case of terrorist organizations with a military structure, the military intelligence (headquarters) organization is more pronounced; in the case of traditional (smaller) terrorist groups, the model of classic intelligence organization (so-called department, bureau, etc.) is more common; for groups with ambitions to apply the so-called cyber-terrorism or terrorism with the use of weapons of mass destruction, the features of the scientific and technological intelligence service, etc., are noticeable. In smaller groups, almost all members (in some way) perform an intelligence-security function; "specialization" for these activities is noticeable in larger groups and organizations (Mijalković 2010, 103-105).

CONCEPT OF INTELLIGENCE SERVICE

The intelligence service is a specialized organization of the state apparatus that uses specific methods and means to carry out intelligence-informative, security and subversive activities, with the aim of protecting national security and realizing national strategic goals, as well as protecting its own interests. Therefore, in addition to intelligence activities (gathering intelligence data on the secrets of the adversary with the aim of realizing vital national interests), security activities (counterintelligence activities to protect the secret data of one's own country, protect vital state bodies and institutions and prevent the actions of the adversary's intelligence services on the domestic territory; protection of the constitutional order; security of certain persons and facilities and counter-terrorist operations), intelligence services also apply the so-called subversive actions that are often connected to the use of force in international relations (Mijalković 2015, 206). The primary task of intelligence institutions is intelligence activity, which represents "the overall planned and controlled action of state authorities on the collection, processing and distribution of information about the power and plans of foreign states, organizations and persons, which may threaten the security of subjects and the values they protect" (Ronin 2009, 13). Intelligence activity is carried out for the purpose of collecting intelligence information that ensures the creation of internal and international policy, as well as for the purpose of collecting information that ensures the implementation of defined political guidelines. More specifically, intelligence information can help political decision makers to: 1. define national interests, 2. develop a coherent national security policy and military strategies, 3. define doctrines and strategies of the armed forces and other security institutions, 4. prepare for national crises and adequately respond to them, 5. prepare in a timely manner responses to all threats to the state and its population (Geneva Centre for the Democratic Control of Armed Forces [DCAF] 2017, 2). As for the security role of the intelligence services, it includes the protection of its own capacities abroad, located in residencies. Capacities are first of all: professional members who manage and implement intelligence activity, agency network through which information is obtained, means of communication, technique and conspiratorial facilities used in operational work, etc.

Intelligence services are institutions of the state institution, and in order to make their operation as efficient and effective as possible, given the specific nature of the tasks they deal with, it is necessary to have a greater part of functional independence compared to other state bodies. This degree of independence depends on whether the specific agency is defined as central (autonomous – directly subordinated to the executive power) or departmental, civil or military, offensive or defensive, national or specialized (financial-economic, energy, technical-technological, political, military- security).

The previously mentioned variety of intelligence services results in frequent mixing of intelligence and security institutions, where the sign of equality is not infrequently put in between, and where again there are clear convergences and divergences. Both intelligence and security institutions have tasks to collect information and to fight against certain forms of threats, usually on a preventive basis. What, among other things, makes the difference between these institutions are: the scope of work, the rules by which they act, the area of action and the specificity of the methods of action. In most cases, intelligence services are offensive institutions that collect classified information and conduct subversive activities in a conspiratorial manner abroad. In contrast, security services as a broader term inclusively include counterintelligence services, which oppose such activities.

The intelligence service is defined as a specialized, relatively independent institution of the state apparatus, authorized to, by legal public and secret means and methods, collect important intelligence data and information about other countries or its institutions and possible internal opponents of one's own country, necessary for conducting the country's policy and undertaking other procedures in peace and war, to implement part of the state and political goals of the country with its own activity, independently or in cooperation with other state bodies (Stajić 2021, 231). Although it is relatively independent in its work, it is necessary for the intelligence service to cooperate with other intelligence-security and similar institutions, which is why it is part of the security-intelligence system, which has clearly defined control and coordination elements. Precisely the control and coordination elements, in addition to the technical-technological, personnel, operational and material financial capacities of the intelligence service, play a very important role in achieving results. However, without previously clear and precise strategic and tactical orientations of the services, which are defined by the highest state authorities, an irrational use of the aforementioned resources would occur.

METHODS OF OPERATION OF INTELLIGENCE SERVICES

The intelligence service, regardless of its place and role in the intelligence-security system of the country, performs complex and specific jobs and tasks. That is why a different approach to classifying its forms of action is visible in the professional literature. Some authors believe that there are three forms of action: intelligence, counterintelligence and subversive. Unlike them, others claim that intelligence services have a specific methodology that includes two groups of activities: intelligence and subversive (Trbojević 2017, 321). Therefore, intelligence services have two types of activities: intelligence-informative and non-intelligence, i.e. subversive.

The first type implies the collection of precise, timely, verified and complete intelligence information about political and security situations, their bearers, relevant for the protection of vital values and the realization of the national interests of the home state, and informing political decision makers, and the second, the implementation of non-intelligence activities (psychological- propaganda, secretly helping political subjects in another country, organizing and carrying out individual acts of violence, etc.) with the same goal.

Intelligence data can be collected in different ways and using different methods, among which the most effective are:

1. Data collection using human sources (HumanIntelligence – HUMINT);
2. Technical methods (Technical Intelligence – TECHINT);
   a) SIGINT (Signals Intelligence)
   b) MASINT (Measurements and Signature Intelligence)
   c) IMINT (Imagery Intelligence)
   g) GEOINT (Geospatial Intelligence)
   d) ITINT (Information Technology Intelligence).
3. Collection of intelligence data from open/public sources (Open Sources Intelligence – OSINT);
4. The investigative method;
5. Method of secret monitoring and observation;
6. Method of international cooperation.

When choosing a method of action, services are guided to the greatest extent by the principles of the most useful, safest and most economical method. The choice of methods in a specific case also depends on technical-technological, financial-material and personnel possibilities. All these methods cannot exist independently of each other, nor does the intelligence service rely exclusively on one method, which is why it is necessary to combine and complement each other.

1. HUMINT is the oldest method of intelligence gathering and essentially refers to the type of intelligence that is obtained from human

resources. The HUMINT method has a subjective character because through direct contact between people, in addition to data collection, the source can be directed, studied and motivated (Nomi 2021). The use of other methods often depends on human sources, while on the other hand, this method requires a lot more time than others, and there is also the possibility of disavowing the source as well as its compromise and recruitment from opposing intelligence services.

2. TECHINT is a technical method that includes the collection of intelligence data with electromagnetic, electromechanical, electro-optical, or bio-electronic sensors, from the earth, sea and atmosphere (Bajagić 2015, 176). This method consists of several collection disciplines, the most important of which are:

a) SIGINT is a method of gathering information obtained by analysing signals and communications between targets of an intelligence attack. SIGINT has two main fields: COMINT – collection of information through interception of communications between individuals or groups and ELINT – collection of information through access to electronic signals. The main difference between COMINT and ELINT is that COMINT signals contain speech or text (telephone or email communication), while this is not the case with ELINT (JEMEnginering 2021).

b) MASINT is a method of performing quantitative and qualitative analysis of data on an object or phenomenon, obtained from various technical and technological sources and their emission, which include: radar sources, audio sources, nuclear sources, radio-frequency sources, electromagnetic sources, laser sources, radiation sources, chemical and biological sources, infrared sources (FAS: Intelligence Resource Program 2000). This method enables the detection of the presence, and the identification and determination of the characteristics of the object (Defence Intelligence Agency [DIA] 2022), and the best known among the examples of the MASINT method are the acoustic data or signatures of military vessels and the weapons they carry, which can be detected underwater using sonar (Encyclopedia of Espionage 2023).

v) IMINT is a method based on image collection through satellite imagery, aerial photography, infrared, lasers, multispectral sensors and radar. Images from the mentioned sources are usually subsequently submitted to the competent authorities, who then analyse them, while some image collection systems can directly transfer images to the operation centre, which allows the images to be used in real time, that is, as soon as possible (GlobasSecurity 2023).

g) GEOINT is a method of producing information from the analysis of images and data, which are related to a specific geographic location, with the aim of examining and evaluating human activity and other natural or social processes anywhere on Earth. Images, data derived from images and geospatial information is now considered an element of GEOINT (Murrett 2006, 10). GEOINT is a broad field that encompasses the intersection of geospatial data with social, political, environmental and numerous other factors. The intelligence community defines GEOINT as the use and analysis of geospatial information to assess geographically relevant activities on Earth (USC Dornsife 2006).

d) ITINT, i.e. the collection of intelligence data using modern information technology, is considered the latest discipline of the technical method, which implies the application of the most modern technological achievements in the field of informatics in order to collect important intelligence knowledge. This discipline has two basic aspects. The first type involves the collection of data from publicly available (Net-Based – social networks, websites, etc.) information systems (Net Open Sources Intelligence – NOSINT) and secret unauthorized intrusions into protected information systems/computer networks (Hackers Intelligence – HACKING) (Bajagić 2015, 234).

3. OSINT is a method of collecting data from open, that is, publicly available sources. This is about data that is available to the public directly or on the basis of a person's request, where a complex and detailed classification of essential from non-essential data is necessary, followed by their processing, analysis and evaluation. The most famous OSINT sources are: legal acts and strategic documents; books and publications; newspapers, magazines and publications; data of competent state bodies for statistics; telephone directories, etc. The advantage of this method of intelligence action is significant intelligence potential, while one of the problems of this method of intelligence action is a large amount of unnecessary data, which, despite the application of various technological tools, still makes it difficult to focus and reach relevant facts.

4. The investigative method is taken as a subtype of the HUMINT method. This method can be used to collect information from persons of intelligence interest such as: defectors, foreign agents, emigrants, travellers and prisoners of war. Information is collected according to strictly established principles by means of various and complex interrogation techniques, that is, through the statements of respondents or through verbal communication with the subject, where the primary

task is to determine the "sincerity" of the person to cooperate, in order to avoid possible disavowals and misinformation. The process of obtaining information in the investigative method does not only mean examining the person, but also requires a combination with other methods such as a survey, interview, document content analysis, polygraph, etc. (Bajagić 2015, 289-293).

5. The monitoring and observation method consists in observing a stationary object or in monitoring individuals. Observation of a stationary object (room, building and open area) is applied in order to: 1. spot visitors, 2. catch the wanted person 3. Process the object for concrete action (Ronin 2009, 48). Special emphasis should be placed on the inspection and observation of the interior of the facility, which is very important for providing the necessary evidence of threatening activity for the purpose of timely preventive or repressive action. On the other hand, the monitoring of the object is carried out for the purpose of: 1. Detailed familiarization with the object for the purpose of possible recruitment, capture, blackmail, discrediting or liquidation, 2. Reaching a wanted person who probably contacts or can contact the object, 3. Discovering the place of gathering groups, 4. Discovering like-minded objects (Ronin 2009, 49). The monitoring of persons is also carried out for the purpose of detection of conspiratorial places where the facility and associates hold meetings or instant meetings, as well as for the purpose of discovering the facility's movement routes during the execution of specific actions.

6. International cooperation between intelligence and security institutions has a very large intelligence potential, and the data obtained through this method often made it possible to stop or intercept certain forms of threats to national security in specific situations. The disadvantage of this method is that the services cannot know what information foreign services kept for themselves during the exchange.

The role of the intelligence services is not limited only to the collection of information, preservation of national security and constitutional order, but often by means of the services, as a very powerful state apparatus, non-intelligence operations are carried out in order to realize the most important political, security, economic and energy interests. Bearing in mind that non-intelligence operations represent the process of realization of decisions based on intelligence product-information, the methodology of carrying out the non-intelligence cycle can be presented in six phases: 1) political-mandatory phase; 2) expert-mandatory phase; 3) planning phase; 4) organizational phase; 5) executive phase; and 6) analytical-report phase (Mijalkovski 2009, 130).

One of the forms of non-intelligence activity is the subversive activity of the intelligence services, which is defined as a systematic, planned, secret and organized activity aimed at changing the situation in other countries in order to strengthen one's own position, which is done in two ways: 1. by providing diverse support to threatened regimes whose policy suits them or 2. by secretly organizing a coup in order to bring like-minded people to power (Stajić 2021, 239). As mentioned, in order to achieve their political and economic interests and intentions, states use intelligence services to implement political coups in other countries. Revolutionary activity requires a previously studied political-security situation, in order to comprehend in which directions revolutionary activities should be directed, and which are the key political, economic and military-security entities that can prevent or hinder their realization. In the actual implementation of the coup, foreign services rely on agency networks in the target state. Also, the key directions of action are the financing and regulation of the policy of the so-called independent media, through which disinformation, propaganda materials and psychological-indoctrination activities are planned.

As part of subversive activities, foreign services form, train and finance paramilitary groups, subversion-terrorist groups, and often plan, organize, assist or personally carry out assassinations of important state officials, who have the authority to make strategic decisions.

In the context of the above, we assess that non-intelligence operations can generally be divided into four groups: a) information-propaganda operations; b) political operations; c) economic operations and g) paramilitary operations. Each of these operations can be performed autonomously or as part of a wider strategy (Trbojević 2017, 327).

Intelligence methods in the fight against terrorism

Terrorist organizations usually plan their activities in headquarters, which in most cases are outside the borders of the country to which the intelligence service belongs. That is why it is considered that the intelligence services are often on the "first line of defence", while the intelligence methods, which are applied at that moment, are of a preventive nature. Intelligence methods collect all data on: 1. historical, strategic and tactical goals of terrorist organizations, 2. intentions and plans, 3. organizational structure (horizontal and vertical), 4. Management and chain of command, 5. Personnel capacities and level of training, 6. Training camps and persons trained in them, 7. Funding sources and financial potential, 8. Countries, organizations or groups that help or encourage the activities of a terrorist organization, 9. Logistics and associates of a terrorist organization, 10. Channels of money, information, people and goods used by terrorist organizations, 11. Technical and technological equipment, 12. Armed potential of terrorist organizations, 13. Criminal involvement of members of terrorist organizations.

Intelligence data collected by intelligence methods can be a good starting point in case of criminal prosecution of the perpetrators of the crime. The intelligence service can, on the basis of the collected intelligence information in a specific case, in accordance with the orders of political decision-makers, carry out certain non-intelligence operations against terrorist groups or send intelligence data about persons or activities to partner services, which further undertake certain (most often repressive) activities.

HUMINT is one of the key methods in the fight against terrorism. Intelligence institutions plan, systematically and conspiratorially create agency positions both among members of the terrorist organization itself, and among persons closely related to its members. Intelligence services recruit those members or collaborators of a terrorist organization with information capabilities, that is, those who can access confidential data or those who can perform certain activities depending on the needs of the service (indicating, recruiting, installing listening devices, etc.). The higher the hierarchical level of a member of a terrorist organization, the intelligence service has a potentially greater chance of success, and if the recruited person is one of the management personnel, the service has the possibility to influence the functioning of the organization itself. The grounds for recruitment can be different, namely: 1. creating friendly relations, 2. compromise, blackmail or intimidation, 3. fraud or misleading, 4. providing financial compensation for activities, etc. A complicating factor in the application of this method is the closedness of terrorist organizations, a high degree of indoctrination and a low degree of interaction with other members of the community. Therefore, the recruitment process itself, as well as the process of reflecting the collaborative relationship itself, must be thoroughly organized and maximally conspiratorial, especially if one takes into account the weight of the potential consequences of deconspiracy. Particularly aggravating circumstances exist in the case of the creation of collaborative relationships in terrorist cells, due to their closedness and isolation, and the finding and recruitment of so-called “lone wolves”.

The HUMINT method is supported by the investigative method, whose potential in the fight against terrorism is enormous, where different methods of investigation are applied, and violence towards the source is often included in the process of obtaining information. Members of terrorist organizations often, as defectors, initiate cooperation with members of the intelligence structures, when by offering the knowledge and information they possess, they usually seek safety and refuge for themselves and their families. Also, members of a terrorist group can, as emigrants or as tourists, attract the attention of intelligence structures, which will use investigative techniques to try to get information that intelligence-interested persons have.

GEOINT and IMINT are methods with great intelligence potential in the fight against terrorism. In order to implement these methods, a significant technical and technological potential of the services and the use of various high-tech devices, drones, airplanes, access to satellite images, etc. is required. Intelligence data obtained by GEOINT and IMINT methods can reveal the location of terrorist bases, training camps or facilities where members of terrorist organizations gather. The independent application of these methods cannot be sufficient for the fight against terrorism, however, the spatial and other data obtained from their application in combination with other indicators for the result can provide the detection of terrorist activity in the early stages (see Brent L. Smith, Jackson Cothren, Paxton Roberts and, Kelly R. Damphousse 2008). In a study published by DNI – OpenSourceCenter, it is stated that by monitoring parameters such as location, timing or frequency of some behaviour, it is possible to predict or observe potential patterns of terrorist activity through the analysis of geospatial intelligence information (Aftergood 2009). Also, the mentioned intelligence data can have an important, and sometimes a key, role in the execution of anti-terrorist military or non-intelligence operations.

The advantages of applying the MASINT method in the fight against terrorism are that qualitative and quantitative results are obtained through physical or chemical analyses of data that can hardly be changed or dissimulated. Thus, for example, by applying this method, in the case of spectroscopic measurement of a leaked chemical bioagent at a specific location, evidence of a potential warehouse of weapons of mass destruction could be collected (The Directorate for Mathematical and Physical Sciences [NSF], and The Intelligence Community 2002, 14) which is a very important field of activity of the intelligence services.

Using radar systems, sonar or radio-frequency systems can determine the identification or presence of terrorist objects at a specific location.

OSINT, as a method related to open sources, can make a huge contribution to identifying terrorist networks and understanding how terrorists use their capacities. Today, there are numerous intelligence tools that enable the rapid identification and flagging of any content deemed to be related to terrorism, allowing for faster analysis and removal from the Internet (Policy Centre for the New South 2022). Also, when a faster analysis of printed texts is enabled, with the analysis of it, it can be quickly determined whether they are propaganda or indoctrination materials, which enables a faster response. The increase in the number of publicly available resources created the basis for the creation of better quality analyses of terrorist organizations and their activities. Collection, classification, processing, analysis and evaluation of newspaper articles, press, books, publications, statistics, available police reports, websites, as well as other national and international public sources can provide information about potential terrorist operations, command structure, propaganda materials, channels of communication and indoctrination, techniques and methodology of action, etc. (U.S. Department of Justice 1999). Publicly available sources often contain a lot of information about charismatic leaders of terrorist organizations, on the basis of which further intelligence or non-intelligence activities can be planned and organized. Through OSINT, information can potentially be obtained about groups, organizations or countries whose support the terrorist organization and its leader enjoy.

SIGINT is one of the most important methods if it is taken into account that more and more communication and correspondence between members of terrorist organizations takes place through modern information technologies. Information that can be disclosed in this way are potentially related to: identity of participants in the conversation, locations from which the conversation takes place, intentions and future plans, potential targets of attacks, financial flows, criminal involvement of terrorists, identification of the target, detection of collaborators or facilitators. Although this is considered to be the second most useful intelligence method (right behind HUMINT), there are two limitations to it: 1. a situation in which terrorists expect that their communication will be intercepted, where in such circumstances those who are trained in intelligence and security will try to disavow the service, 2. the second situation refers to the moment when members of a terrorist organization are prohibited from communicating with each other they use electronic connections (Intelligence functions: Signals Intelligence (SIGINT)) where the intelligence potential, except for some mistakes made by terrorists, is almost non-existent. If communication between members of terrorist groups takes place via electronic communication systems, there are almost always greater or lesser suspicions that they are the target of eavesdropping or interception of communications, which is why they use slang. Continuous eavesdropping and interception of communications and analysis of their content makes it possible to break through slang, after which the language of terrorists becomes clear to the intelligence service. The content that is intercepted by the SIGINT method is often encrypted, which is why intelligence analysis in order to obtain the final intelligence must include various decryption techniques. Important information is also collected through audio and video-audio surveillance devices that are secretly placed inside facilities where terrorists reside, plan or carry out terrorist and non-terrorist activities. These devices are installed by an intelligence or recruited member of a terrorist organization or a person close to its members.

Cyber experts within the intelligence services access the content of communication and the content of computer and mobile devices or other devices used by terrorists in a conspiratorial way, through the HAKING method. The nature of that content may refer to future plans or activities, propaganda material, methods and techniques of action, sources of funding or committed crimes (see the case of Ahmiri Ahmed Azizi and Mohamed Asini: Counter Terrorism Policing 2022). The HACKING method has its application both in the fight against conventional and in the fight against cyber terrorism. One of the most famous hacking software used by intelligence services in the fight against terrorism is the Israeli "Pegasus" (Bergman, Ronen, and Mark Mazzetti 2022).

The method of monitoring and observation is a necessary method in the fight against terrorism. By monitoring a member of a terrorist organization or a person associated with it, information can be obtained about: the terrorist's route, the location of the collection of courier and other packages, places used to conceal persons or weapons, other members of the terrorist group, potential financiers or helpers, targets and the place of execution of the terrorist attacks. In the event of an intention to commit a terrorist act that the service did not expect and it was not detected by applying some other method, this activity can be observed by the monitoring method, and thus the attack can be thwarted.

International cooperation has always been an important segment of the intelligence component of the terrorist campaign, which was particularly intensified after September 11, 2001, and most of the successful operations against al-Qaeda even before this event were the result of joint initiatives and activities. The then director of the CIA told congressional investigators in 2002 that the agency cooperated with numerous European governments, such as Italian, German, French, and British, in order to thwart and destroy terrorist groups (Krstić 2016, 106). Cooperation most often takes place between the intelligence services of friendly countries, however, there are also known examples in which the detection and processing of a terrorist attack occurred solely thanks to data obtained from enemy intelligence and security agencies.[2]

Non-intelligence methods in the fight against terrorism

Based on the previous analysis of non-intelligence methods, it can be concluded that they are implemented in the largest number of cases against other countries and their institutions. However, in order to prevent a terrorist act, intelligence methods are often not enough, which is why it is necessary to eliminate the terrorist threat by applying non-intelligence methods. These methods against terrorism are implemented by the intelligence services through their own intelligence staff, or members of the intelligence network, where sometimes members of terrorist groups themselves are found.

In order to prevent terrorist activity, intelligence services also carry out revolutionary actions in those countries whose regimes support terrorist activity. The very success in these revolutionary activities and regime change would mean the loss of perhaps the most important support for a specific terrorist organization, which would then become an easier target for the intelligence services (Afghanistan). Likewise, intelligence services can carry out special operations against terrorist organizations in those countries whose regimes they seek to protect from the terrorist threat (Syria).

One of the forms of non-intelligence activity of the intelligence services was especially applied in the war against terrorism, which was conducted by the USA in Afghanistan after September 11, 2001. It is

[2] At the end of 2019, the Federal Security Service (FSB) of the Russian Federation detained two persons suspected of preparing a terrorist attack in Saint Petersburg. The FSB previously stated that the arrest was carried out based on information obtained from US authorities.

about the method of targeted killing, which is limited to the specific selection of an individual or individuals, who are wanted for the purpose of liquidation for participating in a terrorist action or belonging to a terrorist group. Before that, the most famous case of targeted liquidation was the pursuit of Black September terrorists by Israeli intelligence after the Olympic Games in Munich in 1972, which took place throughout Europe and the Middle East. The fact is that there is enough evidence that in some of these cases states have decided to act repressively in order to eliminate the perceived terrorist threat. Also, targeted elimination becomes exponentially more important when assessing whether a particular terrorist or terrorist group, at any level, is seeking weapons of mass destruction for execution of a terrorist attack. Individuals likely to rise to the top of the list of candidates for targeted liquidation in this regard include: 1. scientists who provide technical expertise to terrorists in the production or construction of weapons of mass destruction; 2. terrorists known to be actively seeking weapons of mass destruction; 3. terrorists who are known to possess weapons of mass destruction; 4. groups or individuals responsible for the procurement of weapons of mass destruction (Byron Hunter 2009, 15-25). Targeted targets of elimination in the operation of intelligence services can also be objects, that is, movable and immovable things that are extremely important for the operation of terrorist groups, which is why they are attacked using diversionary or related methods. The successful and timely targeted elimination of facilities where weapons of mass destruction are located, i.e. where such weapons are produced or stored, is particularly important.

Non-intelligence action in the form of abduction of persons responsible for a terrorist act is also in the field of action of intelligence institutions, in those situations where deportation or extradition is not possible and when quick action of intelligence authorities is necessary. The kidnapping of members of terrorist groups requires a wide intelligence network and strong logistics because in most cases it is necessary to transfer the abducted person to the territory of another country. Circumstances become even more difficult in the event that the country on whose territory such activity is carried out is positively inclined towards the terrorist group. Kidnappings of members of a terrorist group are carried out in order to hand over the person to the state for questioning, to obtain evidence or to be tried for committed criminal acts.[3]

[3] There are numerous cases of kidnappings by intelligence services, one of the most famous cases being the kidnapping of Abu Omar in Italy (see: Nino 2007).

The subversive action of the intelligence services towards the terrorist organization is carried out in order to eliminate it, weaken it, establish mistrust among its members, achieve paranoia and a sense of insecurity (Despotović i Glišin 2021). The goal of subversive action against a terrorist group is to create and maintain an environment of general insecurity and the disintegration of its most important organizational units. The techniques used by the intelligence service in this case are aimed at members of a terrorist organization, which include: dissemination of compromising material about members of terrorist groups; spreading disinformation about the cooperation of individual members of the terrorist group with intelligence and security institutions; creating an impression among the members of the terrorist group that the person is acting against its interests; dissemination of disinformation about the obstruction of terrorist actions and goals; the use of public information for the distribution of pejorative and compromising content about terrorist leaders. Subversive processes necessarily contain the intention and permanent effort to weaken the terrorist organization more and more, which is achieved, among other things, by intercepting financial supply chains, preventing the supply of necessary equipment and weapons, disabling information channels, etc.

Cyberattack on information and telecommunication systems are one of the effective forms of non-intelligence combat, especially if we take into account the increasing application of information technology in the operation and maintenance of the basic functions of terrorist groups (recruitment, dissemination of propaganda material, sharing of goals and targets, Internet intimidation). By blocking and disrupting communication channels, timely information between members of a terrorist group is prevented or made impossible for a certain period of time, thereby significantly hindering or interrupting terrorist actions (Jevtović 2016). Today's terrorists have realized that the security of the state, as well as the security of the global community, largely depends on computers and information technologies, and that a strategic attack on these systems would have devastating consequences for every country and its economy. Therefore, cyber protection is one of the most important fields of work of the intelligence services, where specific tasks are for the intelligence service to detect and stop the cyber threat in a timely manner (Diaz, Gustavo, and Alfonso Merlos 2008).

CONCLUSION

It is a fact that the absence of a universal concept of terrorism makes the fight on the global level much more difficult, but also opens up space for certain abuses in connection with terrorism and with regard to the specific political and security interests of states. Regardless, states independently or in cooperation with partner countries, define real or potential forms and bearers of threats according to which they direct the action of intelligence institutions. Intelligence institutions in such an environment have no room for a dilemma, because an unequivocal order from the political decision maker clearly defines which organizations or groups have the character of a terrorist threat to the state. The effectiveness of the intelligence services' fight against terrorism depends on: 1. material and financial resources, 2. personnel resources, 3. technical-technological capacities, 4. management staff within the service, 5. control and coordination bodies within the national security system, 6. laws and strategic-doctrinal documents, 7. strategic and tactical orientations, 8. political and security situation in the country, 9. political will of the holder of state power, 10. Methodological concept of struggle.

The methodology of the intelligence agencies' fight against terrorism is an extremely dynamic category, as is the threatening phenomenon itself that needs to be neutralized. The intelligence services have specific organizational units in their composition that deal with the study of both professional practice and scientific theoretical concepts of terrorist activity, in order to constantly improve the methods of combating terrorism. Also, training and specialization of personnel whose task is to oppose terrorism is necessary. The application of one of the defined methods in the fight against terrorism cannot meet the needs of protecting national security, which is why it is necessary to combine and apply several methods in a given situation, in order to produce the best possible results in fighting against terrorism. Also, the intelligence services cannot independently oppose terrorism, but for that, cooperation with other security-intelligence or related institutions is necessary, in accordance with the principle of division of competences between institutions defined by the government. Therefore, it is extremely important to exchange information with partner services and through international cooperation, because so far in several cases it has been shown that it is impossible to oppose terrorism at the national level.

REFERENCES

Aftergood, Steven. 2009. „A GEOINT Analysis of Terorism in Afghanistan."*Federation of American Scientists [FAS].* 3. mart. https://fas.org/blogs/secrecy/2009/05/geoint_terrorism/.

Бајагић, Младен. 2015. *Методика обавештајног рада,* друго, измењено и допуњено издање. Београд: Криминалистичко-полицијскаакадемија.

Bergman, Ronen, and Mark Mazzetti. 2022. „The Battle for the World's Most Powerful Cyberweapon." *The New York Times Magazine*. Jun 28. https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

Brent L. Smith, Jackson Cothren, Paxton Roberts and Kelly R. Damphousse. 2008. „Geospatial Analysis of Terrorist Activities: The Identification of Spatial and Temporal Patterns of Preparatory Behavior of International and Environmental Terrorists." University of Arkansas. 26. februar. https://www.ojp.gov/pdffiles1/nij/grants/222909.pdf.

Byron Hunter, Thomas. 2009. „Targeted Killing: Self-Defense, Preemption, and the War on Terrorism." *Journal of Strategic Security* 2 (2):1-52.

Counter Terrorism Policing. 2022. „Two men convicted of terorrism after digital experts hack devices and find Daesh propaganda." November 3. https://www.counterterrorism.police.uk/two-men-convicted-of-terrorism-after-digital-experts-hack-devices-find-daesh-propaganda/.

Gaćinović, Radoslav. 2016. "Fiksiranje totalitarnog cilja i moć međunarodnog terorizma". *Politika nacionalne bezbednosti*, No. 1/2016, str. 47-66.

Defence Intelligence Agency USA [DIA]. 2022. *MASINT: Measurement and Signature Intelligence*. Washington: Defence Intelligence Agency USA.

Despotović, Ljubiša, i Vanja Glišin. 2021. *Savremeni međunarodni odnosi i geopolitika*. Sremski Karlovci: Kairos.

Diaz, Gustavo, and Alfonso Merlos. 2008. „The role of intelligence in the battle against terrorism on the internet: revising 3/11". *Research Institute for European and American Studies.* January. https://www.files.ethz.ch/isn/48473/rieaspaper117.pdf.

Димитријевић, Војин. 2000. *Тероризам*. Београд: Библиотека: Самиздат.

Encyclopedia of Espionage (Encyclopedia.com). 2023. „MASINT: Measurement and Signature Intelligence". May 5. https://www.encyclopedia.

com/politics/encyclopedias-almanacs-transcripts-and-maps/measurement-and-signatures-intelligence-masint.

FAS: Intelligence Resource Program. 2000. „Measurement and Signature Intelligence (MASINT).” May 8. https://irp.fas.org/program/masint.htm.

Geneva Center for the Democratic Control of Armed Forces [DCAF]. 2017. SSR Backgrounder: Intelligence Services – Roles and responsibilities in good security sector governance. Geneva: Geneva Center for the Democratic Control of Armed Forces.

Global Security. 2023. „Imagery Intelligence.” 13. april. https://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap7.htm.

Intelligence Funcion: Signals Intelligence (SIGINT). 2023. 18. april. https://repository.library.georgetown.edu/bitstream/handle/10822/1041704/GUIX-501-01-14-W7-S4.pdf?sequence=1.

JEM Engenering. 2021. „SIGINT, ELINT and COMINT.” November. https://jemengineering.com/blog-sigint-elint-comint/.

Jevtović, Zoran. 2016. “Uloga društvenih mreža u promociji sajber terorizma”. *Politika nacionalne bezbednosti*, No. 1/2016, str. 99-119.

Кривични Законик Републике Србије. „Службени гласник Републике Србије”. бр. 64/2017, 104/2018 – одлука УС, 15/2021 и 89/2021, Члан 391.

Крстић, Марко. 2016. „Улога обавештајног фактора у борби против тероризма.” *CIVITAS*. 6 (1): 94-116.

Мијалковић, Саша. 2010. „Обавештајне структуре терористичких и криминалних организација.” *НБП: Наука, безбедност, полиција – Журнал за криминалистику и право* 15 (2): 101-114.

Мијалковић, Саша. 2015. *Национална безбедност – треће, измењено и допуњено издање*. Београд: Криминалистичко-полицијска академија.

Мијалковски, Милан. 2009. *Обавештајне и безбедносне службе*. Београд: Факултет безбедности у Београду – Службени гласник Републике Србије.

Милетић, Душан. 2019. „Тероризам као критичан догађај”. Масте рад. Универзитет у Београду: Факултет безбедности.

Murrett, Robert B. 2006. „Geospital Intelligence (GEOINT) – Basic Doctrine”. *Office of Geospital-Intelligence Menagement*. 21. mart. https://irp.fas.org/agency/nga/doctrine.pdf.

Nino, Michele. 2007. „The Abu Omar case in Italy and the effects of CIA extraordinary renditions in Europe on law enforcement and intelligence ac tivities." *International Review of Penal Law* 78 (2007/1-2): 113-141. https://www.cairn.info/revue-internationale-de-droit-penal-2007-1-page-113.htm.

Nomi, Rachele. 2021. „HUMINT: The human intelligence discipline." Grey dynamics, October 23.https://greydynamics.com/humint-the-human-intelligence-discipline/#20_HUMINT_One_of_the_Six_Basic_Collection_Discipline.

Policy Center for the New South. 2022. „OSINT and Counter-Terrorism: Access to Data and (AI) Technologies in Africa." June 15. https://www.policycenter.ma/events/osint-and-counter-terrorism-access-data-and-ai-technologies-africa.

Ронин, Роман. 2009. *Обавештајни рад*. Београд: Службени гласник. Факултет безбедности – Универзитет у Београду.

Симеуновић, Драган. 2009. *Тероризам – општи део.* Београд: Правни факултет.

Стајић, Љубомир. 2021. *Основи система безбедности – са основана истраживања безбедносних појава.* Нови Сад: Правни факултет у Новом Саду. стр. 231.

The Directorate for Mathematical and Fhysical Sciences [NSF], and The Intelligence Comunity. 2002. „Approaches to Combat Terrorism [ACT]: Opportunities for Basic Research." November 19-21. https://www.nsf.gov/attachments/102809/public/ACT.pdf.

Трбојевић, Милован. 2017. „Необавештајни облик деловања обавештајних служби." *Српска политичка мисао* 58 (4/2017): 319-334. doi: https://doi.org/10.22182/spm.5842017.17.

USC Dornsife. 2006. „4 Uses of Geospatial Intelligence." April 15. https://gis.usc.edu/blog/4-uses-of-geospatial-intelligence/.

U.S. Department of Justice. 1999. „Tracking Terorists Through Open Source". 1. april. https://www.ojp.gov/ncjrs/virtual-library/abstracts/tracking-terrorists-through-open-sources.

Weinberg, Leonard. Ami Pedahzur, and Sivan Hirsch-Hoefler. 2004. „The Challenges of Conceptualizing Terrorism". *Terrorism and Policical Violence* 16 (4): 777–794. doi: https://doi.org/10.1080/095465590899768.

Живаљевић, Дргана, иЈуговић, Александар. 2014. „Тероризам као безбедносни проблем и друштвена девијација".*НБП: Наука, безбедност, полиција – Журнал за криминалистику и право* 1 (1): 85-96.

Милован Трбојевић

Факултет за студије безбедности, Универзитет Едуконс, Сремска Каменица

Бранислав Свирчевић

Факултет за студије безбедности, Универзитет Едуконс, Сремска Каменица

МЕТОДЕ ОБАВЕШТАЈНИХ СЛУЖБИ У БОРБИ ПРОТИВ ТЕРОРИЗМА

Сажетак

Адекватна анализа борбе обавештајних служби против терористичких организација захтева приступ који се темељи на методама и средствима деловања обавештајних институција. Тероризам је међу најзаступљенијим безбедносним претњама у медијима и у јавном дускурсу. Све већа бруталност терористичких група и организација, често помињање у јавности и виралност терористичких аката на друштвеним мрежама довели су до тога да се створи специфичан страх према тероризму, због чега је рано откривање и заустављање терористичког деловања од изузетне важности. На пољу превентивног деловања против тероризма најважнију улогу имају обавештајне институције. Обавештајне институције пре свега користе специфичне методе и технике прикупљања података о терористичким претњама чиме се омогућава њихово откривање и пресретање. Поред тога, обавештајне институције се користе и необавештајним методама борбе које захтевају посебну анализу. Са друге стране, терористичке организације, поред извођења терористичких аката спроводе и делатности усмерене на ометање и дезавуисање обавештајних институција, што додатно отежава борбу против тероризма.

Кључне речи: обавештајна агенција, обавештајне методе, необавештајне методе, тероризам, терористичке организација, терористички акт.