

Practical approaches for collecting intelligence information

Ilin Savov

Academy of the Ministry of Interior, Sofia, Bulgaria

ilin_savov@abv.bg

Abstract: *The report examines and assesses the possibilities for obtaining information for the benefit of the security services. The main practical approaches and their specifics regarding the collection of intelligence information are highlighted.*

Keywords: SECURITY, INFORMATION, INTELLIGENCE, OSINT, TECHNICAL TOOLS

1. Introduction

Information has always played a decisive role in the history of civilization and has served as a basis for decision-making at all levels and stages of development of society and the state. In the history of social development can be distinguished several information revolutions related to radical changes in the field of production, processing and transmission of information, which led to radical transformations of social relations. As a result of such transformations, society has acquired in a sense a new quality.

We are witnessing a significant increase in the role, place and impact of information in the life of the individual, society, state. Information today has become a powerful real tangible resource, having even greater value than natural, financial, labor and other resources. Information has become a commodity that is sold and bought. Information in the present plays a paramount role as a non-traditional weapon, information wars arise, develop and end. The cross-border information network Internet is developing and entering our lives extremely fast.

The possibilities for production (creation), processing, storage and dissemination of information are becoming increasingly important. This is not just about the amount of information, ie. for quantity, but also for its qualitative side - structuring and its transformation into knowledge and cognition. In the field of national security, a large amount of information needs to be processed, which is why "the ability of the national information resource to control and form the most important information flows on a regional and global scale must be taken into account.

The development of information and communication technologies covers all spheres of society - economy, social life, culture, science and education, political life. Citizens and society are increasingly relying on reliable and reliable information on the Internet. The state annually increases the number of services and the amount of information it provides to citizens and businesses through the Internet.

This report will briefly look at traditional practical approaches to intelligence gathering.

2. Collection and systematization of intelligence information

Open source intelligence (OSINT) is one of the methods of obtaining information about special services. It includes searching, selecting and collecting information obtained from publicly available sources and its analysis.

According to Central Intelligence Agency (CIA) analyst Sherman Kent, who spoke back in 1947, politicians receive up to 80 percent of the information they need to make peacetime decisions from open sources. Later, General Samuel Wilson, head of the Intelligence Department of the United States Department of Defense from 1976 to 1977, noted that "90 percent of intelligence comes from open sources and only 10 percent is at the expense of the agency." [1]

Open sources include:

- Mass media - newspapers, magazines, radio, television;
- Public government reports, official budget data, collection and analysis of industry reports, press conference materials, various public statements, hearings, legislative debates and speeches;

- Information obtained from professional and academic reports presented at scientific conferences, symposia, professional associations, dissertations and theses and expert reports;
- Professional and academic reports, reports, articles;
- Visits to exhibitions and fairs;
- Internet, in particular social sites, video hosting, directories, blogs, forums

It is necessary to pay attention to another important emphasis on the directions in which the acquisition of information is important in terms of:

- the collection of political, economic and military information necessary for the assessment of the military-economic and moral-political potential of the countries-objects of intelligence activity;
- obtaining special intelligence information related to specific areas of economics, science and technology, military affairs. It is usually intended for a narrower circle of specialists and serves as a material in the development of strategic plans (for economic pressure, for any kind of "sanctions", etc.)

In the practice of all intelligence centers around the world, information obtained by intelligence agents is considered indispensable. This approach remains a crucial tool for overcoming the barriers erected by states to protect national interests. "On the way to getting the most important information ..." Sherman Kent wrote, theoretically justifying the importance of intelligence for the United States ... there are often insurmountable obstacles. They are deliberately created by other countries, and in order to overcome them, methods are needed that are often unfamiliar to the average person. These methods consist of obtaining information by illegal means." [2]

The benefits of intelligence are obvious. Everyone, except the carrier of information, can analyze it, summarize and draw conclusions, ie. to receive the necessary information from the set of indirect data. They are used to solve tasks that are impossible to accomplish, by staff members of the special services or by technical means, difficult or impractical, although this does not preclude their joint work.

Intelligence centers show great interest in the small weaknesses of man, caught in their field of vision and try to use his shortcomings or vices, to deceive him, scare, use, as the German expert J. Yosten writes.

The Internet can be considered an indispensable source of information. The data obtained from the network are used in the field of education, business, medicine, entertainment and recreation, etc. But the Internet is not just an informational Klondike. Cyberspace has long been an arena of network espionage, involving various intelligence agencies and special services working for government, business and the criminal world.

The question arises why the World Wide Web is a space for acquiring foreign secrets? The answer is simple and clear: because the Internet has everything. Everything - this is all information about public and state institutions, organizations, business structures and individuals.

Globalization provides unprecedented access to tools such as the Internet, satellite communications, electronic funds transfer, easy international movement, exchange of official documents and more. Unfortunately, these opportunities are becoming the main tools used by criminal groups and terrorist organizations to achieve their goals. The development of modern global processes makes it possible to connect geographically remote groups, better

coordination, easier communication and realization of information goals.

The Internet is used in various ways by terrorist organizations. They can be combined in two main directions.

The first direction shows that the Internet has become a useful channel of communication that allows terrorists and their followers to spread propaganda and instructions.

The Internet may not be used, but rather attacked by terrorists in the so-called cyber-terrorism. According to many researchers and politicians, who describe the connection between terrorism and the Internet mainly as cyber-terrorism or cyber-war (so-called attacks on communication and computer networks). No less threatening are the numerous Internet applications that terrorists take advantage of.

The information age influences not only the targets and weapons chosen by terrorists and criminal organizations, but also the ways in which these groups work and structure their individual units. Several of the most dangerous terrorist organizations use information technology (IT) - such as computers, software, telecommunications devices, and the Internet - to better organize and coordinate.

The rapid development of equipment and technology in recent decades has led to even faster development of technical means and systems in intelligence. Enormous resources are being invested in the creation of intelligence tools and systems in all developed countries. Hundreds of companies in many countries work in this field. This branch of business has long taken its place in the general system of Western economies and has its own solid legal basis.

All leading experts agree that the value of information in the use of special technical means (electronic surveillance, tracking and eavesdropping) in the investigation of certain forms of serious crime or terrorist acts is unquestionable. This method is extremely important for the protection of national security in modern conditions.

The method "obtaining information through special technical means and channels" covers a set of opportunities and practices.

Conventionally, the method of "obtaining information through special technical means and channels", according to the American classification, is divided into several separate groups:

- Audio surveillance:
 - Eavesdropping on telephone calls;
 - Control of calls made over the Internet (VoIP);
 - Control of conversations in the room.
- Visual surveillance:
 - Hidden video surveillance devices;
 - Built-in video system in vehicles;
 - Surveillance Drones.
- Tracking surveillance:
 - Global positioning systems (GPS systems);
 - Mobile devices;
 - Radio Frequency Identification (RFID) devices;
 - Biometric information technologies (retinal scanning of the eyes when visiting airports, etc.).
- Traffic surveillance:
 - Monitoring of computer information;
 - Monitoring the use of computer systems.

3. Results and discussion

The development of communication technologies on the one hand and their use by people with different interests, including for criminal purposes, has led to the paradox of the world community choosing which priority to be: security or insecurity, security or human rights.

The security dilemma organically stems from the peculiarities of the emerging modern world, including its systemic nature. Therefore, the dilemma of security of man and society is of scientific interest.

There is no doubt that the change of epochs causes a change in the security system: therefore, with the emergence of new dangers and threats, new factors of development, there is a need for a new security paradigm and its security system.

Above all, the definition of the dilemma of security of man and society with a set of values and ideals that change the external and internal environment is indisputable. There are different views here. For example, the basic idea of the US national security strategy is that the establishment of global and, in particular, American security is impossible without America's leadership in the world, without its economic and military superiority over other countries. Hence the strengthening of the role of the state in America's national security system. In other words, it is increasingly viewed through the prism of the triad "individual security - state security - international security" (this model has become particularly important in the light of the events of September 11, 2001). scheme the individual "relinquishes more and more of his care for his own security to the state."

4. Conclusion

Before us is the paradox of modern liberal civilization - the freedom and security of the individual are becoming increasingly dependent on the state, the pressure of the latter on the individual continues to grow, due to the emergence of new information technologies and technical systems that threaten the foundations of the earth. civilization. The dilemma for the security of the individual and the state here is that the distinction between the private and the public is becoming increasingly difficult, and this contributes to the legitimate conquest by the state of the bridgehead "freedom for the individual."

Today, stronger measures need to be taken to combat threats to national security and crime in Bulgaria. An example of this was given by the United States with its Patriot Act of 2001, characterized by a marked increase in the fight against terrorism and a range of restrictions on citizens' rights.

An essential and important ingredient in the fight against crime, creating risks and threats to national security and public order, is the control of traffic data and the use of their unsuspected possibilities for adequate counteraction to any crime.

Each country must proceed from the specific legal and criminal situation in the country, and not simply from abstract notions of "human rights". At the same time, the main condition for the protection of citizens' rights is a strong state power based on law.

5. References

1. **Greene, Kate.** Reality Mining. Sandy Pentland is using data gathered by cell phones to learn about human behavior. – In: *MIT Technology Review* February 19, (2008) <http://www2.technologyreview.com/news/409598/tr10-reality-mining/>
2. **Greenwald, Glenn.** NSA taps in to internet giants' systems to mine user data, secret files reveal. – In: *The Guardian* 6 June (2013). <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>
3. **Kent, Sherman.** Strategic intelligence for American world policy. Princeton University Press, (1966).
4. **Kondratiev, Alexander.** Based on open sources. - In: *Military industrial courier. MIC*, September 16, (2009), № 36 (302)
5. **Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 or the USA FREEDOM Act of 2015.** <https://www.congress.gov/bill/114th-congress/house-bill/2048>
6. **Marks, Paul.** Pentagon sets its sights on social networking websites. - In: *New Scientist* [онлайн]. June 9, (2006) <https://www.newscientist.com/article/mg19025556-200-pentagon-sets-its-sights-on-social-networking-websites/>