

Journal Scientific and Applied Research, Vol. 31, 2026
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

TECHNOLOGICAL CHALLENGES TO THE EFFECTIVE USE OF SPECIAL INTELLIGENCE MEANS

Donika V. Dimanova[1], Silviya K. Kirilova[2]

[1]Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: d.dimanova@shu.bg
[2]Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: silviyakuneva23@gmail.com

ABSTRACT: *The development of information and communication technologies is significantly transforming the environment in which special intelligence means are used. Encrypted communications, virtual private networks, and anonymization technologies limit the effectiveness of traditional methods, while big data analytics, automated processing, and artificial intelligence create new analytical opportunities. The paper examines the impact of the digital environment on the effectiveness of special intelligence means, the role of traffic data, and the possibilities for technological development while ensuring legality and the protection of fundamental rights.*

Key words: *Special intelligence means, Digital environment, Traffic data, Encrypted communications, Data analysis, Artificial intelligence.*

1. Introduction

The development of modern information and communication technologies has a direct impact on the methods used to collect, process, and analyze information in countering crime. The digitalization of communications, the widespread use of Internet-based applications, and the migration of a significant share of communication exchange to encrypted platforms create an environment in which traditional technical methods are increasingly facing substantial limitations [3, 4, 5].

Special intelligence means are, by their nature, intended for the covert collection and documentation of information that cannot be obtained, or can only be obtained with difficulty, through overt methods. Their practical effectiveness, however, directly depends on the nature of the communication environment, the technical capabilities of the implementing structures, and the capacity to process the data obtained [2, 5].

Modern communication platforms use end-to-end encryption technologies that restrict access to the content of exchanged information. In addition, virtual private networks, anonymization services, and other methods for concealing identity and location make it more

difficult to establish communication links and identify the participants involved. These changes require a reassessment of the balance between traditional content interception and the analysis of supplementary information, including traffic data [1, 3, 4].

At the same time, technological development should not be viewed solely as a limitation. The increasing volume of available data and the development of automated analytical tools create opportunities to identify relationships, communication patterns, and behavioral characteristics that would be difficult to detect through traditional manual analysis [3, 6].

The aim of the present paper is to analyze the main technological factors affecting the effectiveness of the use of special intelligence means in the contemporary digital communication environment and to outline opportunities for developing technical and analytical capacity.

To achieve this aim, the methods of analysis, synthesis, comparison, and systematization of regulatory and specialized sources are applied.

2. Exposition

Criteria for assessing the effectiveness of special intelligence means

The effectiveness of special intelligence means should be assessed comprehensively, since their performance cannot be reduced solely to the collection of information. The quality, timeliness, and practical applicability of the data obtained are of substantial importance, as is their role in the prevention, detection, and evidentiary substantiation of criminal activity [5, 6].

Several main criteria can be identified for assessing effectiveness. The first is the ability to collect relevant and timely information that cannot be obtained, or can only be obtained with difficulty, through other methods. This criterion reflects the operational value of special intelligence means and their role in identifying communication links, participants, and mechanisms of criminal activity [2, 5].

A second criterion is their contribution to evidence in criminal proceedings. Information acquired through special intelligence means is significant only when it has been collected and documented in compliance with legal requirements and can be used in the evidentiary process. Therefore, effectiveness should also be considered in relation to the lawfulness of their application and the quality of the evidentiary materials obtained [2, 5].

A third criterion is the capacity to support preventive and operational activities. In many cases, the result of using special intelligence means is not expressed directly in the production of material evidence, but rather in obtaining operationally significant information that supports the planning of subsequent actions and the prevention of criminal activity [5, 6].

The quality of the analysis of the collected information is also of substantial importance. A large volume of data does not in itself guarantee high effectiveness. In the absence of sufficient analytical capacity, the information may remain fragmented, difficult to use, or may fail to enable the timely identification of significant relationships [3, 6].

Resource availability should also be included among the criteria for effectiveness, including technical means, time, human resources, and expert capacity. The use of special intelligence means is a complex process requiring considerable organizational and technological resources; therefore, effectiveness should also be associated with the relationship between the resources invested and the results achieved [5, 6].

Finally, effectiveness cannot be separated from lawfulness and proportionality. A significant information gain cannot be regarded as a positive result if it is achieved through unlawful or disproportionate restrictions on fundamental rights. Therefore, the effective use of

special intelligence means requires both the achievement of an operational result and compliance with the established legal safeguards [2, 5].

These criteria make it possible to regard the effectiveness of special intelligence means as a complex characteristic encompassing operational performance, evidentiary value, analytical usability, resource justification, and lawfulness.

Technological factors affecting the effectiveness of special intelligence means

The effectiveness of special intelligence means cannot be regarded solely as a result of the availability of particular technical tools. It depends on the combined effect of technological resources, the quality of the information obtained, the ability to process it in a timely manner, and the capacity to integrate different information sources [5, 6].

Changes in the communication environment

The spread of Internet-based communication services is gradually displacing traditional telephone communication. Applications such as Viber, WhatsApp, Signal, and Telegram enable the exchange of text, voice, and video messages over Internet infrastructure, with a significant proportion of these communications protected by end-to-end encryption. This limits the effectiveness of traditional telephone interception and directs attention toward other technical and analytical approaches [3, 4]. The analysis of operational methods itself shows that conventional traditional interception of telephone communications has limited applicability to new forms of digital communication.

Encryption does not necessarily eliminate all possibilities for obtaining information, but it changes the nature of the information that can be accessed. When the content itself is unavailable, greater importance is placed on data relating to the communication interaction, such as the time of contact, participants, duration, location, and frequency of communication. This increases the analytical value of traffic data and its importance as a supplementary information resource [1, 3, 4].

Encryption, anonymization, and difficulties in identification

An additional challenge is posed by the use of virtual private networks (VPNs), anonymization services, and communication environments designed to conceal users' technical characteristics and location. In combination with encrypted applications, these technologies can significantly complicate the identification of participants in the communication process and the establishment of links between them [4, 5].

Such an environment places higher demands on technical resources and staff qualifications. It requires the use of combined approaches in which information from different sources is compared and analyzed within a common context. Consequently, the effectiveness of special intelligence means depends less and less on a single method and increasingly on the ability to integrate technical, operational, and analytical information [5, 6].

Increasing volume and complexity of data

Digitalization increases not only the number of communication channels but also the volume of data generated. During prolonged surveillance, substantial amounts of communication, technical, and contextual information may be obtained, the manual processing of which is time-consuming and may result in significant relationships being overlooked.

For this reason, the effectiveness of special intelligence means increasingly depends not only on the collection of information, but also on the ability to structure, filter, and analyze it in a timely manner. Where analytical capacity is insufficient, a large volume of information may become a limitation rather than an advantage for practical effectiveness [3, 6].

Traffic data as a supplementary information and analytical resource

The development of digital communications increases the importance of traffic data as a supplementary source of information in the use of special intelligence means. Unlike communication content, traffic data provide information about the time, duration, participants, technical characteristics, and, in certain cases, location associated with a communication [1, 3, 4]. Their analytical value increases particularly in the context of encrypted communications, where access to content is limited or practically impossible.

Traffic data make it possible to identify communication links and relationships between individuals and objects without necessarily revealing the content of the exchanged information. By analyzing the frequency, sequence, and temporal characteristics of communications, persistent patterns of interaction can be identified, helping to establish the structure and roles within a particular network [3, 4].

Analytical value of traffic data

A key advantage of traffic data lies in the possibility of analyzing relationships between individual communication events. An isolated record of a particular connection has limited informational value, but when multiple records are examined together, recurring contacts, temporal dependencies, changes in communication behavior, and concentrations of interaction among particular participants can be identified [3, 4].

Such analysis is particularly important in countering organized crime, where communication relationships are often distributed among multiple individuals, intermediaries, and technical means. In this context, traffic data can support the identification of key participants, communication hubs, and atypical or intensive interactions [4, 5].

Their analytical value increases further when they are compared with information from other sources. Combining traffic data with results from surveillance, tracking, open sources, or other operational methods makes it possible to build a more comprehensive information picture and verify previously identified relationships [5, 6]. Such an integrated approach reflects the understanding that special intelligence means are most effective when they are not used in isolation, but as part of a broader system for information collection and analysis.

Significance when access to communication content is limited

In the context of end-to-end encryption, traffic data acquire additional importance because they make it possible to analyze the communication pattern itself even when its content remains inaccessible. In this way, the focus shifts from the question of “what was said” to questions such as “who communicated with whom”, “when”, “how often”, and “under what circumstances” [3, 4].

This does not mean that traffic data can fully replace communication content. Rather, they serve a supplementary function by supporting the direction of operational activities, the formulation of hypotheses, and the identification of relationships that can subsequently be verified through other methods [3, 5].

In this sense, their role is particularly important for increasing the informational effectiveness of special intelligence means, as they enable technical and analytical resources to be directed more precisely toward communications and objects of higher operational significance.

Limitations and risks in the use of traffic data

Despite their high analytical value, traffic data should not be regarded as a neutral or risk-free information resource. The accumulation and comparison of large volumes of metadata may enable the development of detailed patterns of behavior, social relationships, and habits, raising issues related to personal data protection and the right to privacy [1, 3].

For this reason, their use should be based on clear legal grounds, purpose limitation, and control over access, storage, and subsequent use of the information. The growing analytical

power of modern information systems makes compliance with the principles of necessity and proportionality particularly important in the processing of traffic data as well [1, 2].

For a clearer distinction between the two main types of information, Table 1 presents a comparison.

Table 1. Comparison between communication content and traffic data

Criterion	Communication content	Traffic data
Main information	Content of exchanged messages	Data on participants, time, duration, and technical parameters
Analytical value	Identification of specific content and intentions	Identification of links, patterns, and communication structures
Impact of encryption	Severely limited by end-to-end encryption	Remains accessible in certain cases
Main application	Establishing and evidencing specific facts	Analysis of relationships and support for operational activities
Main risk	Intrusion into the content of private communications	Profiling and disclosure of behavioral patterns

In summary, traffic data represent an important supplementary information resource whose value increases in the context of encrypted communications and an increasingly complex digital environment. Their effectiveness is most evident when they are analyzed in combination with other information sources; however, their use should be accompanied by adequate safeguards for lawfulness, proportionality, and personal data protection.

Technological opportunities for enhancing effectiveness

The development of information technologies creates new opportunities for increasing the effectiveness of the use of special intelligence means. Although the contemporary communication environment poses a number of challenges related to encryption, anonymization, and the growing volume of data, the same technological processes also provide tools for faster structuring, processing, and analysis of information [3, 5, 6].

Of particular importance is the development of systems for processing large volumes of data. The use of special intelligence means often generates a substantial amount of information of different types, including communication records, traffic data, temporal dependencies, and other digital traces. The application of automated analytical tools makes it possible to process this information more rapidly and systematically, creating conditions for identifying relationships that would be difficult to detect through manual analysis [3, 6]. Such technologies have the potential to enhance analytical capacity in processing information acquired through special intelligence means.

Big data analysis and automated processing

Big data analysis technologies enable the simultaneous processing of multiple information sources and the identification of recurring patterns. This is particularly important in cases of prolonged surveillance, where individual communication events may have limited value on their own but, when compared over time, may reveal persistent links between particular individuals or objects [3, 4].

Automated processing can support the sorting and prioritization of information by directing attention toward events and relationships of higher analytical significance. In this way, the risk of important information elements remaining unnoticed within large datasets is reduced, while the efficiency of the human resources involved is increased [5, 6].

Another important advantage is the possibility of integrating different categories of information. Comparing traffic data with temporal, spatial, and other operational indicators can support the development of a more comprehensive picture of the communication relationships under examination [3, 4].

Artificial intelligence and machine learning

Artificial intelligence and machine learning represent promising areas for expanding the capabilities for processing information acquired through special intelligence means. These technologies enable automated pattern detection, information classification, and identification of anomalies in large datasets [5, 6].

The application of such technologies should not be regarded as a replacement for expert judgment. Rather, they should be used as tools to support analysis by reducing the volume of information requiring manual processing and directing attention toward potentially significant relationships.

Integrated information systems

Another significant factor in increasing effectiveness is the development of integrated information systems. Such systems can provide centralized registration, structuring, and tracking of information related to the different stages of the use of special intelligence means, as well as improved coordination among the institutions involved [5, 6].

These systems can help reduce duplication of information, shorten processing time, and improve the traceability of individual information flows. At the same time, they create conditions for applying more complex analytical models to more structured datasets.

A key condition for the effectiveness of such solutions is their information security. The centralization of sensitive data increases the need for strict access control, logging of activities, protection against unauthorized use, and clearly defined rules for the storage and destruction of information [2, 5].

Development of professional and analytical capacity

Technological modernization cannot lead to a sustainable increase in effectiveness without the parallel development of human resources. Working with modern analytical systems, large datasets, and automated tools requires specialized knowledge and skills in both technical and analytical fields [5, 6].

Training is therefore necessary to combine an understanding of technical capabilities with awareness of legal restrictions and the principles of fundamental rights protection. Only through such a combination can technological capacity be used effectively and lawfully.

In summary, increasing the effectiveness of the use of special intelligence means increasingly depends on the ability to combine technological and analytical solutions. Big data analysis, artificial intelligence, integrated information systems, and the development of specialized expert capacity can significantly improve the processing and interpretation of acquired information. Their use, however, should be governed by clear legal and organizational rules ensuring the protection of sensitive data and fundamental rights.

3. Conclusion

The contemporary digital communication environment is significantly changing the conditions under which special intelligence means are used. The widespread use of encrypted platforms, anonymization technologies, and diverse Internet-based communication channels limits the effectiveness of traditional methods and requires the application of more complex technical and analytical approaches.

The growing importance of traffic data indicates that effectiveness increasingly depends not only on access to communication content, but also on the ability to analyze communication links, temporal dependencies, and behavioral patterns. In this context,

automated processing, big data analysis, artificial intelligence, and integrated information systems create new opportunities for enhancing analytical capacity.

Technological development, however, cannot be considered separately from regulatory and organizational requirements. Increasing effectiveness should be based on a combination of technical capabilities, qualified human resources, adequate mechanisms for information protection, and compliance with the principles of lawfulness, necessity, and proportionality. Only such an integrated approach can ensure the sustainable development of the system for the use of special intelligence means in a dynamically changing technological environment.

References

[1] Electronic Communications Act. Promulgated, State Gazette, No. 41 of 22 May 2007; last amended, State Gazette, No. 66 of 21 July 2026. https://lex.bg/en/laws/ldoc/2135553187.

[2] Special Intelligence Means Act. Promulgated, State Gazette, No. 95 of 21 October 1997; last amended, State Gazette, No. 51 of 5 June 2026. https://lex.bg/laws/ldoc/2134163459.

[3] Savov, I. The Role and Significance of Information and Traffic Data. Sofia: Diomira, 2022.

[4] Savov, I. The Truth about Traffic Data, or How to Use Them Successfully in the Fight against Crime. Sofia: Diomira, 2023.

[5] Stoichkov, O. Special Intelligence Means and Security Services. Sofia: Ciela, 2023.

[6] Hristov, V., Savov, I. Management and Functioning of Security Services. Plovdiv: University of Security and Economics (VUSI), 2016.