DOI: 10.55643/fcaptp.2.67.2026.5176

Vasyl Franchuk
D.Sc. in Economics, Professor, Research Laboratory of OSINT Studies and Security Analytics, Lviv State University of Internal Affairs, Lviv, Ukraine;
ORCID: 0000-0001-5305-3286

Stepan Melnyk
D.Sc. in Economics, Professor, Faculty No. 2 for Educational and Research Activities, Lviv State University of Internal Affairs, Lviv, Ukraine;
ORCID: 0000-0003-3782-5973

Volodymyr Hobela
Candidate of Economy Sciences, Associate Professor of the Department of Management and Economic Security, Lviv State University of Internal Affairs, Lviv, Ukraine;
e-mail: mandos11@ukr.net
ORCID: 0000-0001-7438-2329
(Corresponding author)

Nataliia Shuprudko
Candidate of Economy Sciences, Associate Professor of the Department of Management, Marketing and Logistics, Chernivtsi Institute of Trade and Economics, State University of Trade and Economics, Chernivtsi, Ukraine;
ORCID: 0000-0002-5629-0671

Nila Tiurina
Candidate of Economy Sciences, does not have of the Department of Management and Administration, Khmelnytskyi National University, Khmelnytskyi, Ukraine;
ORCID: 0000-0003-1337-1460

Received: 05/02/2026
Accepted: 02/04/2026
Published: 30/04/2026

DEVELOPMENT OF THE SECURITY ENVIRONMENT: A CONCEPTUAL OSINT MODEL AND MANAGEMENT FRAMEWORK

ABSTRACT

The main purpose of this study is to develop theoretical and conceptual provisions that reveal the essence and mechanisms of security environment development, as well as the role of OSINT and management in this process. The article substantiates the author's approach to interpreting the management of security environment development. Within this framework, the security environment is understood as a condition of human, organizational, societal, and state activity in which real threats exist and the consequences of their impact or counteraction are manifested.

The authors argue that the security environment can be conventionally divided into two levels: unsafe and safe, and propose qualitative criteria for this differentiation. Such division enables understanding of development as an orderly and purposeful transition of the environment to a qualitatively safer state. Accordingly, the development of the security environment is defined as a process of change ensuring its transition to a more secure condition and reproducing its qualitative properties in line with the needs of actors operating within it.

The article substantiates that OSINT represents a form of security activity (a technological process) involving the search, analysis, and transformation of open-source information into targeted intelligence. A structural model of OSINT is proposed, consisting of systemic organizational and technological elements and an action algorithm that together form a unified technological process. OSINT is used to obtain targeted information about threats or their sources within the security environment through detection mechanisms.

The authors propose a theoretical and conceptual model of OSINT utilization in security environment development and management, integrating the key components of this process. The research contributes to the theoretical and practical understanding of the development of national and global security environments and may be useful for scholars, policymakers, practitioners, and public officials, particularly in the context of the russian–Ukrainian war.

Keywords: security environment, financial and economic security of Ukraine, security environment development, security activities, threat, danger, crisis, OSINT

JEL Classification: H56, D83, O38

INTRODUCTION

The human, organizational, and national environment plays a decisive role in ensuring life activity, functionality, and overall sustainability. This environment simultaneously contains various challenges, risks, threats, crises, and hazards, while also providing the conditions, opportunities, and mechanisms to counter them. However, there are situations where protective mechanisms are absent or ineffective, either due to external circumstances or specific territorial constraints, both locally and across Ukraine as a whole. This raises an important conceptual question: how should this part of the life environment be defined?

In political discourse, public administration, and expert discussions, the term security environment is frequently used, yet with varying interpretations depending on the user's

understanding. In academic circles, the search for a clear conceptualization of its essence and structure remains ongoing (Bohdanovych et al., 2021; Bocharnikov & Sveshnikov, 2019; Buhaichuk, 2023; Hlushchenko, 2023; Kryvoruchko et al., 2023; Reznikova, 2022). The security environment is dynamic — it can evolve both positively and negatively. From the perspective of security studies and management, such transformations should be purposeful and structured, gradually shifting the environment from a dangerous to a safer state, that is, toward development. Nevertheless, theoretical and practical approaches to defining its content remain diverse and sometimes inconsistent (Borysenko, 2022). Consequently, the concepts of security environment development and its management continue to be subjects of scholarly inquiry and professional debate.

Parallel discussions have emerged around Open-Source Intelligence (OSINT) — a field concerned with obtaining and processing information from publicly available sources to identify threats, crises, and other security-relevant phenomena (Hayes & Cappa, 2018; Konieczny, 2025; Lakomy, 2023; Sampson, 2017; Van Beek & Rietjens, 2024; Van Puyvelde & Tabárez Rienzi, 2025; Wagner et al., 2019; Yamin et al., 2022; Zaporozhchenko, 2023; Hlavatska et al., 2024, etc.). Numerous scientific studies, professional trainings, and conferences have been devoted to OSINT applications in the security domain. Yet, a clear understanding of how OSINT contributes to the development of the security environment remains underexplored.

Given this context, a significant research gap persists regarding the management of security environment development. There is a lack of a coherent theoretical and conceptual framework that would systematically define the content of the security environment, the essence and mechanisms of its development, and the principles of managing this process. Moreover, the functional role of OSINT within the development of the security environment remains insufficiently clarified, as does the question of whether OSINT should be regarded as a technology or as a type of security activity. These deficiencies substantiate the need for a comprehensive scientific study aimed at bridging the identified conceptual and methodological gaps.

LITERATURE REVIEW

The term security environment has become increasingly popular and is widely used by policymakers, civil servants, experts, academics, journalists, and practitioners. However, scientific literature presents diverse approaches to interpreting its meaning. A number of scholars define the security environment primarily through the set of factors influencing the level of protection of individuals, social groups, organizations, and the state. Yet, these definitions often fail to clarify the direction of such influence — whether it is constructive or destructive.

For instance, Bocharnikov and Sveshnikov (2019) define the security environment as "a set of external and internal relations among active forces across all domains of national security, as well as the conditions, factors, and circumstances that influence or may influence those relations". Reznikova (2022) considers it as "a complex of factors relevant to a particular territory or to Ukraine as a whole, which affect the level of protection of civilians, government bodies, local authorities, and business entities". Similarly, Hlushchenko (2023) views it as "a set of factors that influence the level of protection of people, social groups, and the state within a given territory".

Another line of thought interprets the security environment as the coexistence of both favorable conditions and threats in various spheres of life and relations, affecting the interests of the individual, society, and the state, as well as the mechanisms of protection from such threats. These definitions, however, tend to be overly complex and lack conceptual clarity. For example, Bohdanovych et al. (2021) describe the security environment as "the geopolitical, political-diplomatic, military, and informational domains where favorable conditions or dangerous phenomena, potential and real threats to national interests arise, exist, accumulate, or manifest themselves — domains in which the state implements its national security policy, interacts with international security structures, partners, and institutions to ensure sustainable development within a given time frame".

A third conceptual approach defines the security environment as a set of critical conditions for life activity that must be protected from threats. For instance, Kryvoruchko et al. (2023) define it as "a set of factors — conditions, relations, and events — that delineate the boundaries of potential or real threats to national interests, influence the protection of vital interests of individuals, society, and the state, and determine the degree of protection from internal and external threats". Buhaichuk (2023) emphasizes that it consists of "critically important conditions of state existence that determine its level of protection against external and internal threats".

An analysis of these definitions reveals conceptual similarities despite differences in wording. None, however, fully captures the dual essence of the term's security and environment. Security does not merely imply the absence of threats, but also

DOI: 10.55643/fcaptp.2.67.2026.5176

the presence of effective mechanisms for countering them. This logic should form the basis of a comprehensive definition of the security environment as an integrated and holistic concept.

Like any life-supporting system, the security environment is subject to continuous change influenced by external and internal factors, particularly threats. These changes can be positive or negative, which underscores the need for them to acquire the nature of development. According to Borysenko (2022), development is a process associated with the emergence, transformation, or disappearance of elements and relationships throughout the life cycle of a system to satisfy its own needs and those of its environment. Development involves cyclical reproduction of functions and aims at improving systemic efficiency, which can be positive or negative. Thus, development represents an ongoing process of transformation within socio-economic systems, enabling them to acquire new qualitative properties. In this regard, Borysenko (2022) argues that development must be a managed and repeatable phenomenon to ensure stability — an assertion that is especially relevant to the security environment, where purposeful management is a prerequisite for orderly and directed transformation.

The idea of employing Open-Source Intelligence (OSINT) across various domains — including security and governance – has gained significant scholarly attention over the past decade. Discussions extend from the theoretical and methodological nature of OSINT (as an evolution or "revolution" in intelligence methods) to practical aspects of integrating open-source data into management systems across different levels — from enterprises to national security sectors (Hayes & Cappa, 2018; Konieczny, 2025; Van Puyvelde & Tabárez Rienzi, 2025). Scholars conceptualize OSINT as a process of targeted collection, verification, analysis, and application of open information to support decision-making in contexts of heightened uncertainty (Zhmur, 2022).

Research in security studies and risk management demonstrates that integrating OSINT into threat-identification processes strengthens preventive mechanisms and enhances the quality of risk assessment for business operations and critical infrastructure systems (Hayes & Cappa, 2018). Other scholars identify OSINT as an integral component of Cyber Threat Intelligence (CTI), facilitating knowledge exchange among security actors and laying the foundation for collective defense systems (Wagner et al., 2019). Sampson (2017) explores the use of OSINT in criminal proceedings as a form of "intelligent evidence", emphasizing the need for procedural integrity in data collection, preservation, and presentation.

Since the onset of the russian–Ukrainian war, OSINT has acquired a new vector of development — serving as a tool for real-time monitoring, documentation of war crimes, and in-depth analysis of military operations (Van Beek & Rietjens, 2024; Toma & Vasylova, 2025). At the same time, growing attention is being paid to ethical, legal, and privacy dimensions. Lakomy (2023) highlights dilemmas associated with analyzing online communications of extremist groups, balancing public interest and privacy rights, and mitigating harm from the publication of sensitive data. Konieczny (2025) expands this discussion through the concept of anti-OSINT — reducing digital footprints, preventing data leaks, and strengthening cyber hygiene as means of protecting individuals and organizations from exposure via open sources, which directly affects the architecture of the security environment.

Technological advances in OSINT have been accelerated by the integration of machine learning and big data analytics: automated noise filtering, thematic modeling, and anomaly detection now enable large-scale information processing without compromising analytical quality (Wagner et al., 2019; Zaporozhchenko, 2023). Scholars also stress the need for process standardization, legal expertise, and interagency coordination as prerequisites for the institutional maturity of OSINT research and practice (Van Beek & Rietjens, 2024; Bohdanovych et al., 2021; Hlavatska et al., 2024; Ivkova & Opirskyi, 2025; Martyniuk, 2023).

Other studies address the administrative and legal regulation of open-source information use in national security, delineating the boundaries of permissible data collection, processing, and state oversight (Zhmur, 2022; Martyniuk, 2023; Yarovyi, 2019). A number of scholars interpret OSINT as a component of strategic analysis of security environment development, from continuous external risk scanning and reputational diagnostics to scenario forecasting and evaluation of intervention effectiveness. Within this logic, open data becomes an integral part of risk-oriented management systems, enhancing the adaptability of actors to rapidly changing threat landscapes (Hayes & Cappa, 2018; Van Puyvelde & Tabárez Rienzi, 2025; Wagner et al., 2019).

Yamin et al. (2022) provide a detailed analysis of OSINT tools, interpreting them as the core essence of the concept — a claim that invites critical reflection. Overall, the content analysis of existing research shows that OSINT is examined from multiple scientific perspectives and is used for collecting and analyzing information to support decision-making in various domains. The article argues that OSINT should be conceptualized as a security activity. Accordingly, the structure of OSINT technology and its role in the development of Ukraine's security environment remain underexplored.

AIMS AND OBJECTIVES

The purpose of this study is to develop, on the basis of a systems approach, a set of theoretical and conceptual provisions that reveal the essence and mechanisms of security environment development, as well as the role of OSINT and management in this process.

The main objectives of the research are as follows:

1. To review and analyze scholarly sources relevant to the research topic.
2. To develop a conceptual framework for the notions of "security environment", "development of the security environment" and "OSINT" as a form of security activity, and to propose and substantiate their conceptual content.
3. To design a conceptual model of the structure of OSINT technology and to explicate and justify it as a type of security activity.
4. To elaborate a theoretical-conceptual model of OSINT application and management in support of the development of the security environment.

The results of this research will yield, for the first time, new system-based scientific knowledge of both theoretical and practical significance. These findings can be applied in academic research by expanding the theoretical foundations of security studies – and in practice, through their use in security and management activities aimed at the sustainable development of the security environment.

METHODS

The study employed a comprehensive set of scientific methods, among which the key ones included content analysis, systems approach, concept construction, generalization, comparative analysis, modeling, and expert evaluation.

Content analysis was applied to core security studies concepts — OSINT, security environment, and development of the security environment — which enabled the identification of dominant definitional approaches and revealed inconsistencies that prevent their comprehensive conceptualization. The systems approach and the method of conceptual construction were used to formulate the content of these notions by structuring them into sets of interrelated elements, each having an individual purpose but collectively performing a shared function as an integrated conceptual entity.

Through the method of generalization and comparative analysis, the study identified the informational and detection mechanisms inherent in OSINT and substantiated its classification as a type of security activity. The modeling method was employed to develop a model of the structure of OSINT technology as a form of security activity and a theoretical–conceptual model of OSINT application and management in the development of the security environment.

An expert evaluation was conducted to validate the proposed definitions of security environment, development of the security environment, and OSINT, as well as the fundamental theoretical assumptions, namely:

- whether OSINT constitutes an element of specific types of security activity;
- whether OSINT contains intrinsic information-detection mechanisms;
- whether changes in the security environment occur (a) under the influence of threats that deteriorate it; (b) as a result of countermeasures that improve it; or (c) through the strengthening of security culture, which also enhances it.

The expert panel consisted of seven experts selected according to the following criteria: (1) professional experience in management or security activities, or (2) established academic reputation in the relevant field, particularly with practical knowledge of OSINT.

An expert evaluation form was designed for this purpose, containing the definitions and theoretical statements on the left-hand side and a three-point evaluation scale on the right-hand side ("Yes", "Difficult to answer", "No"). The evaluation procedure comprised four stages:

1. At the first stage, expert forms were distributed individually to allow independent consideration.
2. At the second stage, the authors conducted an online presentation of the proposed concepts, followed by an open discussion.
3. At the third stage, each expert completed the evaluation form by marking one response per statement using the provided scale. The completed forms were then returned to the authors.

DOI: 10.55643/fcaptp.2.67.2026.5176

4. At the fourth stage, the authors analyzed and summarized the collected responses to identify consensus positions and divergences.

This multi-method approach ensured the internal coherence, validity, and practical applicability of the developed theoretical and conceptual models, reinforcing their relevance for both academic and applied security management contexts.

RESULTS

The analysis of scientific sources demonstrated that the environment primarily represents the conditions that ensure human, organizational, and societal life activities. From the standpoint of security, these conditions are influenced by various threats that destabilize or destroy them, causing crises and dangers. In turn, actors within this environment counter such threats by creating and applying corresponding security mechanisms and capabilities, which are reflected in the overall state of the environment – that is, in the quality of life-supporting conditions. This fundamental principle formed the basis for constructing the content of the concept of security environment, which was developed according to the following logic:

1. The content of this concept must reflect the essence of the term environment, interpreted as the conditions in which human life takes place; the set of relations and interactions that define the living context of individuals, organizations, and communities.
2. Human life unfolds under the influence of diverse threats — some of which are the direct consequence of human activity itself. To counter them, the state, society, organizations, and individuals create specific capabilities and mechanisms, thereby engaging in security activity aimed at ensuring protection.

Accordingly, the security environment is defined as the state of conditions of human, organizational, societal, and state life and of the relations among them — both domestically and internationally — where (or with respect to which) real threats exist, and which reflects the consequences of their impact or the results of counteraction against them.

This definition was endorsed by six experts (86%). In current discourse, the term security environment is used to denote the set of critical conditions for life activity, critical relationships within organizations, communities, or states, and the critical state of intergovernmental relations caused by real threats that require adequate countermeasures.

To assess the level of environmental safety, a two-level gradation is proposed:

1. Unsafe environment — conditions of human, organizational, societal, and state life and relations in which threats exert a destructive influence and where no countermeasures exist or are effectively applied, either locally or nationwide.
2. Safe environment — conditions of human, organizational, societal, and state life and relations in which threats are absent, neutralized in time, or compensated for through the restoration of processes, functionality, or integrity, including damage recovery after the impact of a threat.

Based on the authors' conceptual reasoning and expert assessment (71%), it was established that the transition of the security environment from an unsafe to a safe state (and vice versa) occurs under three main conditions:

1. Under the influence of certain threats, which worsen it to the point of a crisis and a dangerous state.
2. As a result of counteraction against threats (security activity), which improves it.
3. Through the strengthening of security culture, which also improves it.

Examples illustrating specific shifts in Ukraine's security environment from a relatively safe to a hazardous state are presented below. In particular, as a result of the russian military aggression against Ukraine, as of November 2024, a substantial number of life-support infrastructure facilities satisfying essential human needs have been destroyed (Table 1). At the time of manuscript preparation, the extent of destruction had further deteriorated; however, updated official statistics have not yet been published.

Table 1. Information on the destruction of key life-support environment facilities in Ukraine as of November 2024. *(Source: developed by authors based on (KSE Institute, 2026))*

Name of the destroyed facilities	Total amount
Residential buildings	236 000
Educational institutions	4 000
Cultural heritage sites	3 921
Religious buildings	399
Sports complexes	343
Healthcare facilities	1 554
Hydropower plants (Kakhovka and Dnipro) and thermal power plants (Trypillia and Zmiiv)	4

Further evidence of the shift of Ukraine's security environment toward a more hazardous state, driven by extensive destruction, is reflected in the dynamics of the aggregate assessment of direct economic losses (Figure 1).

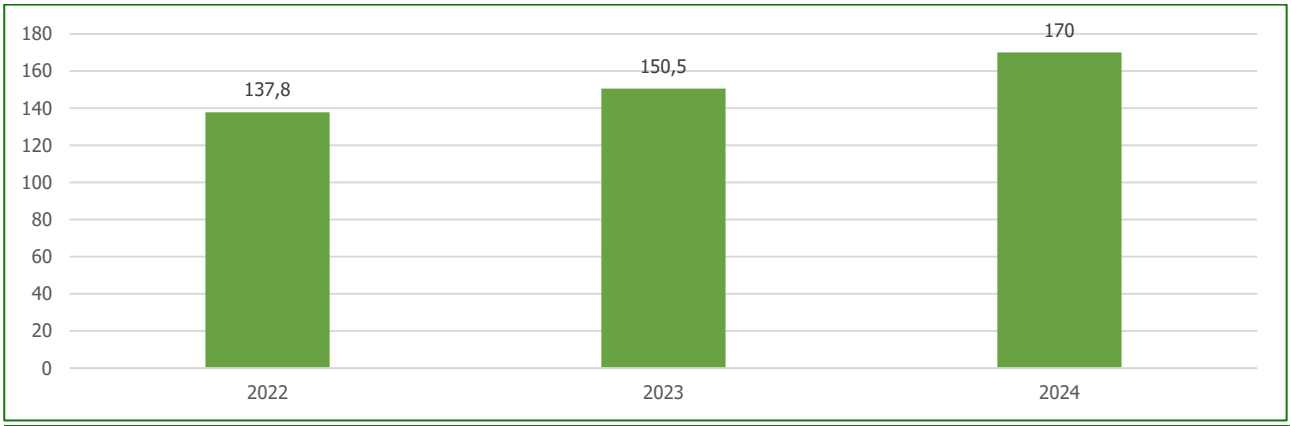

Figure1. Dynamics of the aggregate assessment of direct economic losses in Ukraine, USD billion. *(Source: developed by authors based on (KSE Institute, 2026))*

A further indicative marker of the deterioration of Ukraine's security environment is reflected in the dynamics of public debt over the period 2022–2024 (Figure 2). The data presented in Figure 2 demonstrate that public debt has increased by approximately 2.5 times, thereby posing a threat to Ukraine's economic security.

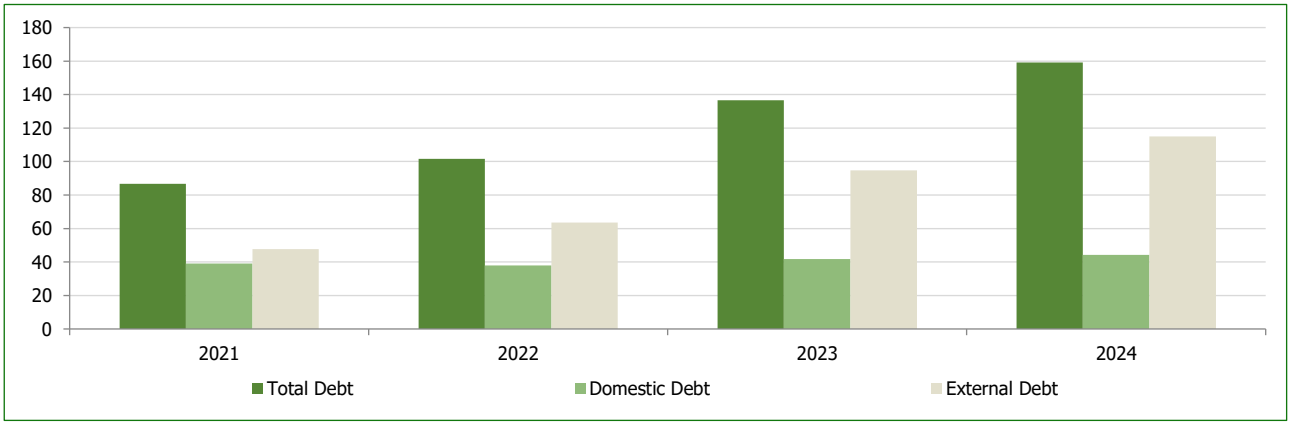

Figure 2. Dynamics of Ukraine's public debt in 2022–2024, USD billion. *(Source: DEVELOPED by authors based on (Minfin, 2026))*

At the same time, changes in the security environment may, and indeed do, occur toward its improvement.

It is essential that the improvement of the security environment be an orderly and managed process, thus acquiring the nature of development. On this basis, and supported by expert consensus (100%), the following definition was formulated: development of the security environment is a process of ordered and purposeful changes within the security environment that ensure its transition to a qualitatively new and safer state.

DOI: 10.55643/fcaptp.2.67.2026.5176

This process implies the reduction or elimination of destructive threat impacts, the restoration of disrupted processes, and the compensation of losses. Such changes result from the performance of various types of security activity — a general collective term encompassing preventive, detection, elimination, and recovery mechanisms embedded across multiple sectors of security practice. For example, detective activities include detection and elimination mechanisms; law enforcement activities — preventive, detection, and elimination mechanisms; and insurance activities — recovery and compensation mechanisms.

Within this framework, OSINT (Open-Source Intelligence) is classified as a type of security activity, as it inherently contains detection mechanisms that combine technological and procedural components to collect and analyze open-source information about threats and to document unlawful activities across time and space. Thus, in terms of its mode of implementation, OSINT constitutes a form of security activity. This view was supported by five experts (71%).

Through OSINT, relevant information from open sources — especially social networks — can be collected rapidly using both free and paid analytical tools. This includes information related to the distribution of narcotics and weapons, the identification of dangerous groups or individuals, cyber threats, and cases of commercial information leakage by company employees, among others.

Contemporary OSINT, as a form of security activity, represents an integrated technological process characterized by a complex structure composed of essential elements, which are grouped into two categories: organizational–technological components and an operational algorithm (Figure 3).

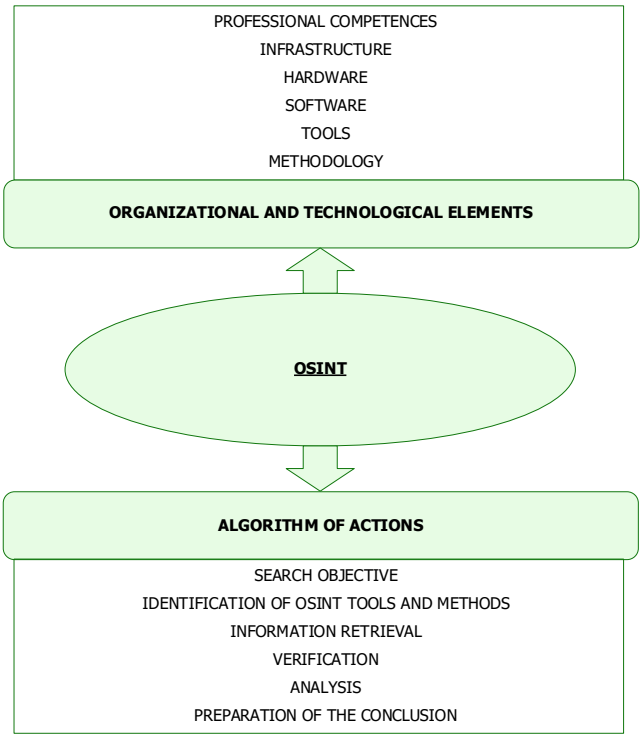

Figure 3. Conceptual model of the structure of OSINT technology as a form of security activity.

In this regard, OSINT, in terms of its substantive content, constitutes a technology that integrates an action algorithm, infrastructure, competencies, methods, and tools required for the search, analysis, and transformation of relevant information from open sources into targeted information. This interpretation of OSINT content is supported by six experts (86%).

Accordingly, OSINT represents a form of security activity (a technological process) encompassing the search, analysis, and transformation of relevant information from open sources into targeted information.

Based on this definition, OSINT as a security activity is employed for the acquisition, analysis, and conversion of information obtained from open sources into targeted information. At the same time, it should be emphasized that such information is taken into account in decision-making processes aimed at addressing tasks across various types of security activities, including operational-search activities, law enforcement activities, detective work, investigative activities, internal service

investigations, journalistic investigations, financial investigations, searches for missing persons, searches for stolen property, and related fields.

The use of OSINT within other types of security activity for gathering necessary information constitutes a component of that activity, thereby forming a conditionally technologically unified process (Figure 3). This reasoning was endorsed by five experts (71%). Importantly, the effectiveness of OSINT application does not depend on who performs it — whether it is conducted by the subject of a given security activity or by an external specialist.

For example, in the event of a breach of banking secrecy, an internal security department may conduct an investigation using its own OSINT capacities or outsource the task to an external expert. In both cases, the objective remains the same: to collect and analyze open-source information regarding the possible transmission of confidential data by a suspected employee to a third party. Thus, OSINT operates simultaneously as a component of the bank's internal security (detective) activity and as an independent type of security activity that contains detection mechanisms.

Consequently, using OSINT — either as a stand-alone type of security activity or as a detection mechanism embedded in other forms of security work — enhances the capability of relevant actors to obtain information about threats (their identification) or about those who perpetrate them. This, in turn, strengthens the capacity to prevent, neutralize, or eliminate such threats and to hold perpetrators accountable. In this way, OSINT contributes directly to the development of the security environment at organizational, community, regional, and national levels, in the economic and financial spheres in particular.

The effectiveness of security environment development largely depends on the quality of management activity performed by the responsible entity. Managerial decisions ensure the targeted influence over various types of security activity — including OSINT — resulting in the reduction or elimination of destructive threats and the restoration of disrupted processes or compensation for incurred losses.

Management activity, however, is not exercised in general terms but through specific types of activities or within particular organizations where various forms of security-related work are performed. It is implemented through the core management functions — planning, organizing, motivating, and controlling — as well as through the connecting processes of communication, decision-making, and leadership. Therefore, management of the development of the security environment is, first and foremost, the management of particular types of security activity, within which managerial decisions are prepared and implemented. These decisions are developmental in nature — that is, they are intended to produce structured and purposeful changes in the security environment leading to its transition to a safer state.

Examples of such managerial decisions include:

- planning — approval of a security plan that defines a set of tasks and measures aimed at preventing threats, mitigating their destructive power, eliminating their consequences, or restoring affected processes;
- organizing — assignment of security functions to units or institutions (at both organizational and national levels) and approval of functional responsibilities;
- motivating — establishment of reward systems, such as bonuses or moral incentives, for achieving specific security-related performance indicators;
- controlling — approval of audit schedules and performance reports.

The decision-making process involves active communication among organizational units, officials, and experts to collect relevant information, accompanied by leadership influence that strengthens coordination and facilitates the adoption of final managerial decisions. Information about the state of the security environment is collected by specialists within various types of security activity, particularly through OSINT, depending on the nature of the threats. The data obtained are then used for preparing and implementing operational decisions aimed at preventing, mitigating, or eliminating threats, as well as for restoring disrupted functions or compensating for damages. Additionally, such information supports the broader communication and coordination processes required for making managerial decisions that guide the ongoing development of the security environment.

To better understand the role of OSINT and management in the development of the security environment, we have developed a theoretical and conceptual model of this process (Figure 4).

DOI: 10.55643/fcaptp.2.67.2026.5176

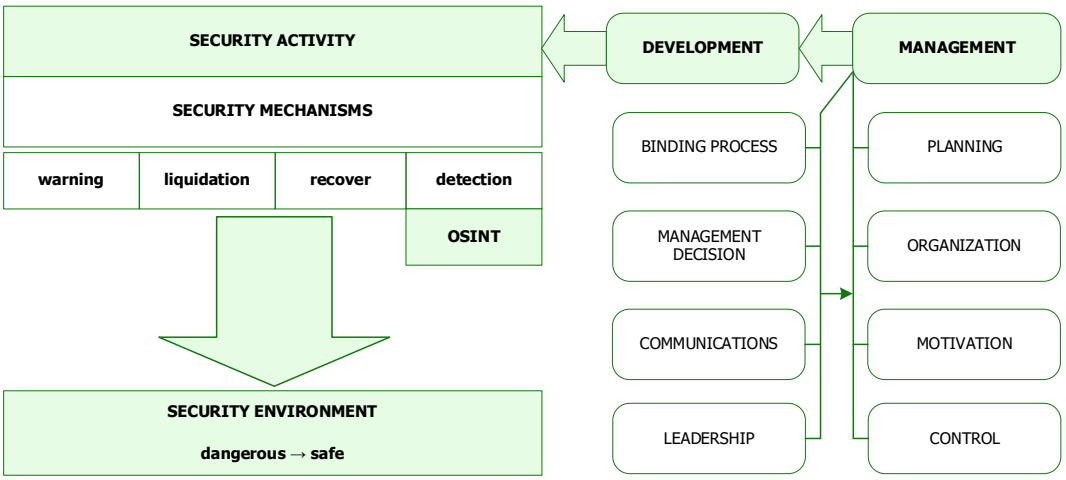

Figure 4. Theoretical conceptual model for use in developing and managing a security environment.

DISCUSSION

The use of a combination of different scientific methods in the present study made it possible to generate new knowledge and to refine existing understanding of the management of security environment development as an integrated process, as well as the role of each element within this activity. Given the theoretical nature of the research, the obtained results require appropriate interpretation in the form of scholarly discussion.

Based on the analysis of academic sources (Bohdanovych et al., 2021; Bocharnikov & Sveshnikov, 2019; Buhaichuk, 2023; Hlushchenko, 2023; Kryvoruchko et al., 2023; Reznikova, 2022), it has been established that definitions of the concept of the "security environment" are predominantly reduced to conditions and factors that destabilize the environment or to spheres and relationships in which threats emerge, without specifying whether these threats are potential or actual. However, it is precisely this distinction between potential and actual threats that determines the appropriate mode of action.

The approach to defining the concept of the "security environment" and its classification into security levels is proposed by the authors for the first time and differs substantially from those presented in the aforementioned and other published scientific sources, primarily in terms of content, as well as in the systemic and comprehensive nature of the proposed set of structural elements and criteria. The core emphasis is placed on the understanding of the security environment as, first, a state of living conditions and relations in which (or with respect to which) actual threats occur; and second, a state that reflects the consequences of the impact of actual threats or the counteraction to them.

In contrast to existing approaches (Bohdanovych et al., 2021; Bocharnikov & Sveshnikov, 2019; Buhaichuk, 2023; Hlushchenko, 2023; Kryvoruchko et al., 2023; Reznikova, 2022), this study proposes to distinguish two levels of the security environment — "hazardous" and "safe" — along with corresponding qualitative criteria enabling their assessment. Moreover, compared to the cited publications of other authors, the article provides analytical evidence (Tables 1 and 2, Figure 1) regarding the presence of threats within Ukraine's security environment that contribute to its deterioration. In particular, this concerns the destruction of key life-support environment facilities in Ukraine as of November 2024, the scale of which continues to increase daily as a result of russia's military aggression. The destruction of these and other facilities results in substantial economic losses, which are reflected in the aggregate assessment of direct economic losses that, as of November 2024, increased by USD 32.2 billion compared to 2022. Over the same period, Ukraine's public debt increased by 2.5 times.

Even based on these three groups of criteria and their indicators, it is evident that the security environment in economic and financial sectors is shifting toward a hazardous state, in which the living conditions of individuals, organizations, society, and the state are significantly or completely destroyed (Shkolnyk, F et al., 2022). It is important to emphasize that these changes in living conditions are negative in nature and occur in a chaotic manner.

This example is critically important for understanding the essence of the development of the security environment, the definition of which is proposed in science by the authors for the first time. The content of this concept is interpreted as a process of change — namely, changes that must be orderly and goal-oriented. The direction of this orientation clearly indicates a transition of the environment toward a qualitatively new and safer state, that is, the acquisition of new qualitative properties enabling its reproduction to meet the needs of those who conduct their life activities within this secure

environment. Such an approach to understanding and interpreting the concept of "security environment development" provides new scientific and practical insights into its content and structure.

At the same time, the study concludes that development itself constitutes an internal characteristic and directional orientation of change processes within the security environment that shift it toward a safer state. Changes in the security environment occur as a result of security activities, among which, as demonstrated in this research, OSINT also belongs.

The obtained scientific results expand the established understanding of OSINT beyond its traditional interpretation as merely an intelligence tool or method (Hayes & Cappa, 2018; Konieczny, 2025; Lakomy, 2023; Sampson, 2017; Van Beek & Rietjens, 2024; Van Puyvelde & Tabárez Rienzi, 2025; Wagner et al., 2019; Yamin et al., 2022; Zaporozhchenko, 2023; Hlavatska et al., 2024). This study substantiates that OSINT, in terms of its content, constitutes a technology, as it integrates a specific set of elements presented in Figure 2, while in terms of its form it represents a security activity, as it incorporates detection mechanisms, is directly implemented by a human specialist, and can be applied within various types of security activities to obtain targeted information from open sources. This approach to understanding OSINT is proposed in science for the first time and differs significantly from existing interpretations, as it introduces a conceptual model of the structure of OSINT as a form of security activity.

The research results also expand the views of a scholar (Borysenko, 2022) regarding the necessity of managing development and provide a clear understanding of this process, taking into account the specific content of the concept of "security environment development". In this context, development functions as a characteristic and directional orientation of security tasks and measures implemented within particular types of security activities, including OSINT, aimed at transferring the security environment to a qualitatively new and safer state. Thus, management is effectively carried out through security activities, including OSINT, while managerial decisions that permeate the entire management process are developmental in nature, as they are oriented toward implementing orderly changes to enhance the level of safety of the living environment. This process is illustrated in Figure 4.

This scientific result is particularly relevant when management is considered in its classical sense, that is, as a distinct type of activity aimed at coordinating human efforts and utilizing resources through the application of general management functions and integrative processes to achieve overall organizational goals (1, 2).

In this study, management of the development of the security environment is carried out with the purpose of transferring it to a new, qualitatively safer state. This approach is proposed in science for the first time and enables researchers to apply this model in studies of security environment development management practices, while practitioners may use it to design this process in accordance with established theoretical principles.

At the same time, it should be emphasized that the conducted research has certain limitations. In particular, the obtained scientific results are based on theoretical generalization and expert assessment and are conceptual and methodological in nature; therefore, they require further empirical validation.

CONCLUSIONS

As a result of this research, it has been theoretically substantiated that the security environment should be understood as the state of conditions of human, organizational, societal, and state life and of the relations among them within the country, as well as interstate relations, where (or with respect to which) real threats exist and which reflects the consequences of their impact or of counteraction against them. Its development occurs as a process of ordered and purposeful changes that ensure its transition to a qualitatively new and safer state. This transition — from an unsafe to a safe level — can be assessed using the qualitative criteria proposed for each condition.

The study demonstrates that the development of the security environment takes place through the implementation of various types of security activities, which encompass mechanisms of prevention, detection, elimination of threats, as well as recovery and compensation for losses. Development, therefore, acts as both a characteristic and a directional dimension of security-related objectives and measures. It is substantiated that, from the standpoint of security science, OSINT (Open-Source Intelligence) constitutes a distinct type of security activity, since it contains inherent detection mechanisms that provide target-specific information on threats or their sources to relevant actors. Consequently, OSINT serves as a mechanism for the development of the security environment, enhancing its adaptive and preventive capacity.

In addition, the research proposes a definition of OSINT as a technology and presents a model of its structure, which integrates infrastructural, methodological, and procedural components of open-source data collection and analysis. The study also clarifies the content of security environment management, emphasizing that management of development is

DOI: 10.55643/fcaptp.2.67.2026.5176

achieved through the management of specific types of security activity, including OSINT. The proposed theoretical and conceptual model of OSINT application in the development and management of the security environment provides a comprehensive representation of this process, revealing the interconnections and roles of its constituent elements.

Thus, the formation of a system-based theoretical and conceptual framework makes it possible to reveal the content of the security environment, the essence and mechanisms of its development, and the role of management and OSINT, as a technology, from a security perspective. In doing so, this study helps address, to a significant extent, the existing scientific gap in understanding and managing the development of the security environment under contemporary conditions.

In turn, this opens new conceptual and methodological opportunities for researchers to study the security environment, regional economies — including frontline regions — territorial communities, and related domains. It is also relevant to examine the security environment of Ukraine's financial sector, as well as its military dimension.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Abdulrahaman, M. D., & Alhassan, A. (2023). A case study of Fayol's principles: Classical management theory in contemporary organizations. *International Journal of Management, Technology and Entrepreneurship*, *10*(2), 45–59. https://doi.org/10.1108/IIMTJM-10-2023-0026
2. Ashford, S. J., & George, E. (2023). What Henri Fayol couldn't know: Managing gig workers in the new era. *Business Horizons*, *66*(6), 685–696. https://doi.org/10.1016/j.bushor.2023.06.005
3. Hayes, D. R., & Cappa, F. (2018). Open-source intelligence for risk assessment. *Business Horizons*, *61*(5), 689–697. https://doi.org/10.1016/j.bushor.2018.04.001
4. Konieczny, M. (2025). Anti-OSINT methods ensuring protection of personal data in the context of cybercrime. *RAIP*, *1*(XXV), 127–144. https://doi.org/10.5604/01.3001.0055.1100
5. Lakomy, M. (2023). Open-source intelligence and research on online terrorist communication: Identifying ethical and security dilemmas. *Media, War & Conflict*, *17*(1), 23–40. https://doi.org/10.1177/17506352231166322
6. Sampson, F. (2017). Intelligent evidence: Using open-source intelligence (OSINT) in criminal proceedings. *The Police Journal: Theory, Practice and Principles*, *90*(1), 55–69. https://doi.org/10.1177/0032258X16671031
7. Van Beek, H., & Rietjens, S. (2024). Open-source intelligence in the Russia–Ukraine war. In M. Rothman, L. Pepperkamp, & S. Rietjens (Eds.), *Reflections on the Russia–Ukraine War* (pp. 57–76). Leiden University Press.
8. Van Puyvelde, D., & Tabárez Rienzi, F. (2025). The rise of open-source intelligence. *European Journal of International Security*, *10*(1), 1–15. https://doi.org/10.1017/eis.2024.61
9. Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, *87*, 101589. https://doi.org/10.1016/j.cose.2019.101589
10. Yamin, M. M., Ullah, M., Ullah, H., Katt, B., Hijji, M., & Khan, M. (2022). Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security. *Mathematics, 10*(12), 2054. https://doi.org/10.3390/math10122054
11. Zaporozhchenko, M. M. (2023). Mistse OSINT v zhyttievomu tsykli kiberataky. *Telekomunikatsiini ta informatsiini tekhnolohii*, *1*(78), 53–60. https://doi.org/10.31673/2412-4338.2023.015360
12. Bohdanovych, V. Yu., Iliashov, O. A., Komarov, V. S., & Oleksiiuk, V. V. (2021). Pidkhid do otsiniuvannia bezpekovoho seredovyshcha v suchasnykh umovakh vedennia zbroinoi borotby. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen NUOU imeni Ivana Cherniakhovskoho*, *2*(72), 33–39. https://doi.org/10.33099/2304-2745/2021-2-72/33-39
13. Borysenko, Ya. V. (2022). Terminolohichnyi analiz sutnosti poniattia «rozvytok» yak ekonomichnoi katehorii. *Naukovi perspektyvy. Seriia «Ekonomika»*, *8*(26), 117–131. https://doi.org/10.52058/2708-7530-2022-8(26)-117-131
14. Bocharnikov, V. P., & Sveshnikov, S. V. (2019). *Bezpekove seredovyshche 2030*. Maister Knyh.

15. Buhaichuk, K. L. (2023). Bezpekove seredovyshche derzhavy v konteksti diialnosti Ministerstva vnutrishnikh sprav Ukrainy. *Pravo i bezpeka*, *2*(89), 111–120. https://orcid.org/0000-0003-2429-5010

16. Hlavatska, A., Anhelska, O., & Opirskyi, I. (2024). Doslidzhennia tekhnolohii vykorystannia OSINT yak novoi zahrozy deanonimizatsii osoby v Internet-prostori. *Kiberbezpeka: osvita, nauka, tekhnika*, *1*(25), 19–50. https://doi.org/10.28925/2663-4023.2024.25.1950

17. Hlushchenko, O. O. (2023). Funktsiia zabezpechennia bezpeky derzhavy v umovakh voiennoho stanu. *Chasopys Kyivskoho universytetu prava*, *1*, 53–56. https://doi.org/10.36695/2219-5521.1.2023.10

18. Zhmur, N. V. et al. (2022). Istoriia stanovlennia ta suchasnyi stan OSINT. *Scientific Works of National Aviation University. Series: Law Journal "Air and Space Law"*, *3*(64), 95–101. https://doi.org/10.18372/2307-9061.64.16895

19. Ivkova, V., & Opirskyi, I. (2025). OSINT-tekhnolohii yak zahroza kiberbezpetsi. *Kiberbezpeka: osvita, nauka, tekhnika*, *3*(27), 165–179. https://doi.org/10.28925/2663-4023.2025.27.749

20. Kryvoruchko, I., Shchur, N., & Semenets-Orlova, I. (2023). Kontseptualni zasady rozvytku bezpekovoho seredovyshcha v Ukraini. *Naukovi pratsi MAUP. Politychni nauky ta publichne upravlinnia*, *6*(72), 37–45. https://doi.org/10.32689/2523-4625-2023-6(72)-5

21. Martyniuk, S. O. (2023). Administratyvno-pravove rehuliuvannia zabezpechennia funktsionuvannia OSINT u sferi natsionalnoi bezpeky. *Analitychno-porivnialne pravoznavstvo*, *5,* 355–358. https://doi.org/10.24144/2788-6018.2023.05.63

22. Reznikova, O. O. (2022). *Natsionalna stiikist v umovakh minlyvoho bezpekovoho seredovyshcha*. Kyiv: NISD.

23. Shkolnyk, I., Frolov, S., Orlov, V., Datsenko, V., & Kozmenko, Y. (2022). The impact of financial digitalization on ensuring the economic security of a country at war: new measurement vectors*. Investment Management and Financial Innovations, 19*(3), 119-138. https://doi.org/10.21511/imfi.19(3).2022.11

24. Toma, M. H., & Vasylova, O. V. (2025). Instrumenty OSINT: fiksatsiia voiennykh zlochyniv v Ukraini. *Analitychno-porivnialne pravoznavstvo*, *2,* 905–909. https://doi.org/10.24144/2788-6018.2025.02.134

25. Yarovyi, T. S. (2019). OSINT yak perspektyvnyi instrument kontroliu za lobistskoiu diialnistiu. *Ekspert: paradyhmy yurydychnykh nauk i derzhavnoho upravlinnia*, *4*(6), 201–208. https://doi.org/10.32689/2617-9660-2019-4(6)-201-208

26. KSE Institute. (2026, February 15). *War-related damages have reached USD 170 billion*. https://minfin.com.ua/ua/2025/02/15/145399465/

27. Minfin. (2026, February 15). *Public debt of Ukraine*. https://index.minfin.com.ua/ua/finance/debtgov/

Франчук В., Мельник С., Гобела В., Шупрудько Н., Тюріна Н.

РОЗВИТОК БЕЗПЕКОВОГО СЕРЕДОВИЩА: КОНЦЕПТУАЛЬНА МОДЕЛЬ OSINT ТА УПРАВЛІННЯ

Основною метою дослідження є розробка на засадах системного підходу теоретико-концептуальних положень, які розкривають зміст і механізми розвитку безпекового середовища, а також роль у цьому процесі OSINT та управління. У статті концептуально розкрито й обґрунтовано авторський підхід до розуміння й трактування управління розвитком безпекового середовища. У межах цього підходу безпекове середовище розглянуте як стан умов життєдіяльності людини, організації, суспільства, держави та відносин між ними, де мають місце реальні загрози та відображаються наслідки їхнього впливу або протидії їм.

Автори статті довели, що безпекове середовище умовно поділяється на два рівні — «небезпечне» та «безпечне», а також розробили відповідні якісні критерії його оцінювання. Такий поділ є важливим для розуміння сутності розвитку безпекового середовища, яке має змінюватися впорядковано й спрямовано. Відтак розвиток безпекового середовища — це процес змін, які забезпечують його перехід у якісно новий безпечніший стан. Доведено, що розвиток відбувається внаслідок виконання відповідних видів безпекової діяльності та є внутрішньою характеристикою й спрямуванням цього процесу змін.

У статті розширене усталене розуміння OSINT як інструмента чи методу розвідки та запропоновано розглядати його як технологію й вид безпекової діяльності. OSINT як технологія поєднує інфраструктуру, компетентності, методи та інструменти, необхідні для пошуку, аналізу й перетворення відомостей із відкритих джерел на цільову інформацію. Запропонована модель структури OSINT передбачає два пов’язані блоки: системні організаційно-технологічні елементи й алгоритм дій, які утворюють технологічний процес. OSINT як вид безпекової діяльності містить механізми виявлення, цю модель використовують для отримання цільової інформації з відкритих джерел.

У дослідженні обґрунтовано зміст управління розвитком безпекового середовища. Доведено, що цей процес відбувається шляхом управління видами безпекової діяльності, зокрема OSINT, а розвиток виступає характеристикою та спрямуванням безпекових завдань і заходів. Автори статті розробили теоретико-концептуальну модель використання OSINT у розвитку безпекового середовища та управління ним.

DOI: 10.55643/fcaptp.2.67.2026.5176

Наукова розвідка буде корисна для науковців, практиків, державних службовців та інших суб'єктів безпекового середовища, особливо в умовах російсько-української війни.

Ключові слова: безпекове середовище, фінансова та економічна безпека України, розвиток безпекового середовища, діяльність у царині безпеки, загроза, небезпека, криза, OSINT

JEL Класифікація: H56; D83, O38