

Electronic scientific and practical journal
**INTELLECTUALIZATION OF LOGISTICS
AND SUPPLY CHAIN MANAGEMENT**

#38(2026)
August '26



WWW.SMART-SCM.ORG

ISSN 2708-3195

DOI.ORG/10.46783/SMART-SCM/2026-38



Electronic scientific and practical publication in economic sciences

Electronic scientifically and practical journal "Intellectualization of logistics and Supply Chain Management" included in the list of scientific publications of Ukraine in the field of economic sciences (category "B"): **Order of the Ministry of Education and Culture of Ukraine dated June 11, 2026 No. 928 (Appendix 13 item 205).**

Cluster: Economic Transformation, Business and Administration

Specialties: C1 – Economics and International Economic Relations (by specializations)

D3 – Management

D5 – Marketing

ISSN 2708-3195

DOI: <https://doi.org/10.46783/smart-scm/2026-38>

The electronic magazine is included in the international scientometric databases:

Index Copernicus, Google Scholar

Released 6 times a year

№ 38 (2026)

August 2026

Kyiv - 2026

Founder: Viold Limited Liability Company

Editor in Chief: Hryhorak M. Yu. – Doctor of Economics, Ass. Professor.

Technical editor: Harmash O. M. – PhD (Economics), Ass. Professor.

Assistant editor: Davidenko V. V. – PhD (Economics), Ass. Professor.

Members of the Editorial Board:

BUGAYKO Dmytro – Doctor of Economics, Professor, Academician of the Academy of Economic Sciences of Ukraine, Corresponding Member of the Transport Academy of Ukraine;
RELAWATI Rahayu – Doctoral Degree, Professor;
KRAUS Nataliia – Doctor of Economics, Professor;
MOSKVICHENKO Iryna – PhD in Economics, Associate Professor;
ILCHENKO Nataliia – Doctor of Economics, Professor;
GALKIN Andrii – Doctor of Technical Sciences, Professor;
ROMANENKOV Yuri – Doctor of Technical Sciences, Professor;
SIMONETTI Biagio – PhD, Associate professor;
SOKOLOVA Olena – PhD in Economics, Associate Professor;
HLYNSKYI Nazar – Doctor of Sciences in Economics;
LIESKOVSKÁ Vanda – Doctor of Sciences in Economics, Professor;
SHKURENKO Olga – Doctor of Economics, Professor;
LAZORENKO Larysa – Doctor of Sciences in Economics, Professor;
ALKEMA Viktor – Doctor of Economics, Professor;
ZAPOROZHETS Oleksandr – Doctor of Technical Sciences, Professor
DYMA Oleksandr – Doctor of Economics, Associate professor

The electronic scientific and practical journal is registered in international scientometric data bases, repositories and search engines. The main characteristic of the edition is the index of scientometric data bases, which reflects the importance and effectiveness of scientific publications using indicators such as quotation index, h-index and factor impact (the number of quotations within two years after publishing).

In 2020, the International Center for Periodicals (ISSN International Center, Paris) included the Electronic Scientific and Practical Edition "Intellectualization of logistics and Supply Chain Management" in the international register of periodicals and provided it with a numerical code of international identification: ISSN 2708-3195 (Online).

Recommended for dissemination on the Internet by the Academic Council of the Department of Logistics NAU (No. 7 of February 26, 2020). Released 6 times a year. Editions references are required. The view of the editorial board does not always coincide with that of the authors.

Electronic scientifically and practical journal "Intellectualization of logistics and Supply Chain Management" included in the list of scientific publications of Ukraine in the field of economic sciences (category "B"): *Order of the Ministry of Education and Culture of Ukraine dated June 11, 2026 No. 928 (Appendix 13 item 205).*

Cluster: Economic Transformation, Business and Administration

Specialties: C1 – Economics and International Economic Relations (by specializations); D3 – Management; D5 – Marketing

DOI: <https://doi.org/10.46783/smart-scm/2026-38>
e-mail: support@smart-scm.org

facebook.com/Smart.SCM.org
тел.: (063) 593-30-41
<https://smart-scm.org>

Contents

INTRODUCTION

7

HRYPHORAK M.Yu. Doctor of Economics, Associate Professor, Professor of the Department of International Business and Logistics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine), **KARPUN O.V.** PhD (Economics), Associate Professor, Associate Professor of Department of International Business and Logistics, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute» (Ukraine)

INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT: CONCEPTUAL FRAMEWORK, RESEARCH AGENDA, AND THE ROLE OF A SCIENTIFIC JOURNAL

8– 35

GURINA G.S. Academician of the Academy of Sciences of Ukraine, Doctor of Economics Science, Professor, Vice Rector of Kyiv University of Law of the NAS of Ukraine (Ukraine), **PODRIEZA S.M.** Academician of the Academy of Sciences of Ukraine, Doctor of Economics Science, Professor (Ukraine), **PODRIEZA M.S.** Doctor of Philosophy in Economics State University «Kyiv Aviation Institute» (Ukraine)

TRANSFORMATION OF ORGANIZATIONAL CULTURE AND MANAGEMENT MODELS IN INTERNATIONAL BUSINESS UNDER THE INFLUENCE OF INNOVATION AND GEOPOLITICAL CHANGES

36 – 43

HARMASH O.M. PhD (in Economics), Associate Professor Department of International Business and Logistics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (Ukraine), **MARCHUK V.YE.** Doctor of Technical Sciences, Professor, Professor of the Department of International Business and Logistics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine), **DAVYDENKO V.V.** PhD of Economics, associate professor, associate professor of the department of Industrial Marketing, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine)

A DIGITAL EARLY-WARNING FRAMEWORK FOR MONITORING THE ECONOMIC SECURITY OF DEFENCE-INDUSTRIAL ENTERPRISES

44 – 66

SIBRUK V.L. PhD in Economics, Docent, Associate Professor of Industrial Marketing Department National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine), **SUVOROVA I.M.** PhD in Economics, Docent, Associate Professor of Industrial Marketing Department National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute. " (Ukraine), **YARMOLIUK O.Ya.** PhD in Economics, Docent, Associate Professor of Industrial Marketing Department National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute. " (Ukraine)

MERCHANDISING TRANSFORMATION UNDER THE INFLUENCE OF TECHNOLOGICAL, COMPETITIVE AND CONSUMER FACTORS: A COMPREHENSIVE CONCEPT FOR RETAIL

67 – 79

DRANUS V.V. PhD in Economics, Associate Professor, Associate Professor of the Department of Finance and Credit, Petro Mohyla Black Sea National University, Mykolaiv (Ukraine), **DRANUS L.S.** PhD in Economics, Associate Professor, Associate Professor of the Department of Management, Petro Mohyla Black Sea National University, Mykolaiv (Ukraine), **PROKOPYSHYN O.S** PhD in Economics, Associate Professor, Associate Professor of the Department of Accounting and Taxation, Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies Lviv (Ukraine)

INFORMATISATION AND DIGITALISATION OF BUSINESS PROCESSES AS TOOLS FOR THE STRATEGIC MANAGEMENT OF LOGISTICS ACTIVITY AND SUSTAINABLE DEVELOPMENT OF TRADE ENTERPRISES

80 –88

DABIZHA V.V. PhD in Public administration, Associate Professor, Associate Professor of the Department of International Relations and Political Consulting, HEI “Open International University of Human Development “UKRAINE” (Ukraine), **NEKRIACH A.I.** Doctor of Political Science, Professor, Professor of the Department of International Relations and Political Consulting, HEI “Open International University of Human Development “UKRAINE” (Ukraine)

ARTIFICIAL INTELLIGENCE IN THE ACTIVITIES OF THE SECURITY AND DEFENSE FORCES OF UKRAINE: PUBLIC AND ADMINISTRATIVE ASPECT

89 –99

VOLSKA O.M. Doctor of Science in Public Administration, Professor, Professor of the Department of Public Administration and Local Self-Government, Kherson National Technical University, Khmelnytskyi, (Ukraine)

ARTIFICIAL INTELLIGENCE AS A TOOL FOR ENHANCING THE GOVERNANCE CAPACITY OF UKRAINE’S SECURITY AND DEFENCE FORCES

100–110

SOROKIVSKA O.A. Doctor of Economics, Professor, Ternopil Ivan Puluj National Technical University Ternopil (Ukraine)

INTERNATIONAL INFORMATION SECURITY IN THE CONTEXT OF THE EMERGENCE OF A GLOBAL INFORMATION SOCIETY

111 –121

TRUSHKINA N.V. Ph.D. (in Economics), Senior Researcher, Senior Research Officer of the Sector of Industrial Policy and Innovative Development of the Department of Industrial Policy and Energy Security, Research Center for Industrial Problems of Development of the NAS of Ukraine (Ukraine)

SCENARIO MODELLING OF INVESTMENT NEEDS FOR THE RESILIENT RECOVERY OF UKRAINE’S CRITICAL INFRASTRUCTURE: STRATEGIC PATHWAYS UNDER WARTIME AND POST-WAR RISKS

122 –147

SPORYSHEV K. O. Doctor of Science in Public Administration, Associate Professor, Deputy Head of the Educational and Scientific Institute for Training of Management Personnel in Scientific Work – Head of the Scientific and Research Laboratory of Construction and Operational Application of the National Guard of Ukraine, National Academy of the National Guard of Ukraine, (Ukraine), **BONDARENKO O. H.** Doctor of Science in Public Administration, Associate Professor Head of the Logistics Management Department of the Educational and Scientific Institute for Management Training, National Academy of the National Guard of Ukraine (Ukraine)

"SAFE CITY" AS A SECURITY COMPONENT OF THE SMART CITY CONCEPT: PUBLIC AND MANAGEMENT ASPECT

148 –161

GRABOVSKIY D.Y. Postgraduate Student National University "Kyiv Aviation Institute" (Ukraine), **BUGAYKO D.O.** Doctor of Science (Economics), Professor, Academician of the Academy of Economic Sciences of Ukraine, Corresponding Member of the Transport Academy of Ukraine, Instructor of ICAO Institute, Leading Researcher, Professor (Full) of the Logistics Department National University "Kyiv Aviation Institute" (Ukraine)

OPTIMIZATION OF UKRAINE-EU LOGISTICS ROUTES UNDER WARTIME RISKS

162 –168

UDC 351.86:004.8:005.21
JEL Classification: H56, H83, O33.

Received: 2026-07-18
Accepted: 2026-08-28
Published: 2026-08-30

Volska O.M. Doctor of Science in Public Administration, Professor, Professor of the Department of Public Administration and Local Self-Government, Kherson National Technical University, Khmelnytskyi, (Ukraine)

ORCID – 0000-0001-5047-4579
Researcher ID
Scopus author id: – 57201896051
E-Mail:

ARTIFICIAL INTELLIGENCE AS A TOOL FOR ENHANCING THE GOVERNANCE CAPACITY OF UKRAINE'S SECURITY AND DEFENCE FORCES

Olena Volska "Artificial intelligence as a tool for enhancing the governance capacity of Ukraine's security and defence forces". The article examines artificial intelligence as a tool for enhancing the management capacity of Ukraine's security and defence forces. It is substantiated that, under conditions of increased risk, time constraints, incomplete information, adversarial interference and rapidly changing operational environments, the effectiveness of the relevant actors largely depends on the speed of data processing, the quality of forecasting, the coordination of actions and the timeliness of management decisions. The authors propose defining the management capacity of Ukraine's security and defence forces as the comprehensive ability of the relevant authorities, military formations and other actors within the security and defence sector to exercise their statutory powers through the timely acquisition and analysis of information, risk assessment, threat forecasting, activity planning, coordination, and the adoption and implementation of management decisions. Its structure comprises institutional, information and analytical, forecasting, planning, coordination and adaptive capacities, as well as the capacity to adopt and implement decisions. The article presents an AI-supported management cycle encompassing data acquisition, information verification and integration, situational analysis, threat identification, risk assessment, forecasting, the development of courses of action, decision-making and monitoring of decision implementation. The information and analytical, monitoring, forecasting, planning, coordination, resource optimisation and control functions of AI, together with its decision-support function, are systematised. It is emphasised that artificial intelligence should not be regarded as an autonomous management actor but as an information, analytical and forecasting tool supporting the activities of authorised actors. Effective AI application requires a human-machine interaction model in which algorithmic capabilities are combined with professional experience, critical thinking, contextual understanding and human legal responsibility. Final decision-making and responsibility for its consequences must remain with the competent official.

Keywords: artificial intelligence, management capacity, security forces, defence forces, security and defence sector, public administration, management decisions, threat forecasting, situational awareness, human-machine interaction



Олена Вольська «Штучний інтелект як інструмент підвищення управлінської спроможності сил безпеки і оборони України». У статті досліджено штучний інтелект як інструмент підвищення управлінської спроможності сил безпеки і оборони України. Обґрунтовано, що в умовах підвищеного ризику, обмеженого часу, неповноти інформації, протидії противника та швидкої зміни оперативної обстановки ефективність діяльності відповідних суб'єктів значною мірою залежить від швидкості оброблення даних, якості прогнозування, узгодженості дій і своєчасності прийняття управлінських рішень. Запропоновано авторське визначення управлінської спроможності сил безпеки і оборони України як комплексної здатності відповідних органів, військових формувань та інших суб'єктів сектору безпеки і оборони реалізовувати визначені законом повноваження шляхом своєчасного отримання й аналізу інформації, оцінювання ризиків, прогнозування загроз, планування діяльності, організації взаємодії, прийняття та реалізації управлінських рішень. У її структурі виокремлено інституційну, інформаційно-аналітичну, прогностичну, планувальну, координаційну, адаптаційну спроможності та спроможність до прийняття і реалізації рішень. Представлено управлінський цикл використання ШІ, що охоплює отримання, перевірку й об'єднання даних, аналіз обстановки, виявлення загроз, оцінювання ризиків, прогнозування, розроблення варіантів дій, прийняття рішення та контроль його виконання. Систематизовано інформаційно-аналітичну, моніторингову, прогностичну, планувальну, координаційну, ресурсно-оптимізаційну, контрольну функції ШІ та функцію підтримки прийняття управлінських рішень. Наголошено, що штучний інтелект має розглядатися не як самостійний суб'єкт управління, а як інструмент інформаційно-аналітичної та прогностичної підтримки діяльності уповноважених суб'єктів. Встановлено, що результативне використання ШІ потребує формування моделі людино-машинної взаємодії, за якої алгоритмічні можливості поєднуються з професійним досвідом, критичним мисленням, контекстуальним розумінням і юридичною відповідальністю людини.

Ключові слова: штучний інтелект, управлінська спроможність, сили безпеки і оборони, сектор безпеки і оборони, публічне управління, управлінські рішення, прогнозування загроз, обороноздатність, ситуаційна обізнаність, людино-машинна взаємодія.

Introduction. The contemporary security environment is characterised by dynamism, uncertainty, the simultaneous emergence of threats of different types, and a rapid increase in the volume of information required for management decision-making. In the context of the full-scale armed aggression against Ukraine, the ability of the security and defence forces to obtain, process, and analyse data in a timely manner, forecast developments, coordinate the activities of relevant actors, and promptly make well-founded decisions is of particular importance.

Under such conditions, traditional management mechanisms do not always ensure the necessary speed of information processing and response to threats. Large volumes of heterogeneous data, information

received from numerous sources, rapid changes in the operational environment, and the need to coordinate the activities of different components of the security and defence sector create a demand for the implementation of modern information and analytical technologies. One such technology is artificial intelligence, whose capabilities make it possible to automate certain information processes, identify patterns in large datasets, assess risks, model possible scenarios, and provide information support for management decision-making.

The use of artificial intelligence in the activities of the security and defence forces is not limited to the development of new weapons, military equipment, unmanned systems, and autonomous systems. An



equally important area is the direct application of AI in management activities, including information collection and analysis, monitoring of the security environment, threat forecasting, operational planning, resource allocation, coordination of interagency interaction, and the preparation of management decision alternatives.

In this context, artificial intelligence should be regarded as a tool for enhancing the management capacity of Ukraine's security and defence forces. This refers to the ability of the relevant actors to exercise their legally defined powers, identify threats in a timely manner, assess risks, ensure effective planning, organise interaction, and make well-founded decisions under conditions of limited time, uncertainty, and information overload.

According to the Law of Ukraine "On National Security of Ukraine", the security forces and defence forces encompass a broad range of military formations, law enforcement and intelligence agencies, and other public authorities whose activities are aimed at protecting Ukraine's national interests. At the same time, these actors differ in their legal status, functional purpose, competence, organisational structure, and the nature of the tasks they perform. Therefore, the implementation of AI in their activities requires not only appropriate technological support but also a coordinated management approach that takes into account the specific characteristics of each actor, ensures the interoperability of information systems, and facilitates effective data exchange.

The importance of this research is further reinforced by the fact that artificial intelligence can simultaneously improve the quality of management and generate new risks. The use of algorithmic systems is associated with the possibility of erroneous or biased outputs, insufficient algorithmic transparency, dependence on data quality, cyber threats, risks of unauthorised access to information, and uncertainty regarding

responsibility for decisions prepared or made with the use of AI.

Particular attention should be paid to determining the appropriate balance between algorithmic support and human decision-making. Artificial intelligence should contribute to improving the speed and soundness of management processes without removing humans from the assessment of the situation or from responsibility for the final decision. This approach is consistent with NATO's Principles of Responsible Use of AI in Defence: lawfulness; responsibility and accountability; explainability and traceability; reliability; governability; and bias mitigation.

Ukraine has already established a general strategic framework for the development of artificial intelligence. The Concept for the Development of Artificial Intelligence in Ukraine identifies national security and defence among the priority areas for the application of relevant technologies, while the Action Plan for 2025–2026 provides for the further implementation of its provisions. At the same time, the existing policy documents do not provide a comprehensive understanding of how AI should be integrated specifically into the management processes of the security and defence forces, which management functions should be supported by algorithmic systems, or what criteria should be applied to assess the effectiveness of their use.

Therefore, scientific consideration is required not only of the technological capabilities of AI but, above all, of its place within the system of public and military management, its impact on the management capacity of the security and defence forces, the limits of its use in the preparation and adoption of decisions, and the conditions under which the application of relevant technologies can contribute to strengthening Ukraine's defence capability.

Analysis of recent research and publications. The use of artificial intelligence in the security and defence sector has been

studied by foreign and Ukrainian scholars, primarily in the context of automating military processes, developing command-and-control systems, deploying autonomous systems, analysing operational information, and supporting decision-making. S. Alon-Barkat and M. Busuioc examine the interaction between humans and algorithmic systems in public-sector decision-making. In their research, they draw attention to the risk of "automation bias", whereby public officials may uncritically rely on algorithmic recommendations, as well as to the selective adherence to such recommendations. Their findings are important for determining the limits of AI use in the management activities of security and defence forces. B. Boudreaux, M. Ashby, F. Morgan, A. Lohn and other scholars have systematised the principal areas of military AI application and characterised the associated ethical, operational and strategic risks. The researchers emphasise that achieving a technological advantage requires the simultaneous introduction of risk-mitigation mechanisms and the responsible use of

In Ukrainian academic literature, O. Nikoliuk, O. Rodina and T. Savchenko identify the principal areas of artificial intelligence application in the development of management solutions in public administration. T. Pshenychna examines the integration of artificial intelligence technologies into public administration. O. Harmash, T. Fedorenko and O. Hvozdoва investigate information and analytical support, cyber-risk monitoring and assessment, substantiating the need to transform cyber-threat data into a basis for clear and well-founded management decisions.

Thus, the existing studies provide a theoretical foundation for understanding the technological, security and ethical aspects of artificial intelligence application. At the same time, the public administration dimension of this issue remains insufficiently explored, particularly the impact of AI on the overall

capacity of Ukraine's security and defence forces to perform information and analytical, monitoring, forecasting, planning, coordination and other management functions.

The formulation of the goals of the article. The purpose of the article is to provide a theoretical substantiation of the role of artificial intelligence in enhancing the management capacity of Ukraine's security and defence forces, to systematise its key management functions and areas of application, and to identify the organisational and institutional conditions for the effective use of AI technologies in monitoring, forecasting, planning, coordination, and management decision-making support processes.

Presentation of the main results. The study of artificial intelligence as a tool for enhancing the management capacity of security and defence forces requires, first and foremost, clarification of the meaning of the concept of "management capacity". In the academic literature, capacity is generally associated with a particular actor's possession of the necessary powers, organisational structure, and human, financial, informational and technical resources that enable the achievement of defined objectives and the performance of assigned tasks [9].

Management capacity cannot be reduced exclusively to the formally established competence of a particular authority. The existence of legally defined powers does not in itself guarantee the ability to exercise them effectively in practice. Such capacity depends on the quality of management processes, the professionalism of personnel, access to reliable information, the speed of communication, the effectiveness of interagency cooperation, and the ability to adopt and implement decisions in a timely manner.

Management in the security and defence sector is distinctive because it is carried out under conditions of increased risk, time constraints, incomplete information,



adversarial interference and rapidly changing operational environments [10]. Errors or delays in management processes may cause not only organisational or material losses but also directly affect human lives, the resilience of state institutions, territorial integrity and national defence capability.

Security forces and defence forces constitute interconnected but functionally distinct components of the security and defence sector. Pursuant to the Law of Ukraine "On the National Security of Ukraine" [3], security forces comprise law enforcement and intelligence agencies, state bodies with special-purpose law enforcement functions, civil protection forces and other bodies entrusted with ensuring national security. Defence forces include the Armed Forces of Ukraine, as well as other military formations, law enforcement and intelligence agencies entrusted with ensuring national defence [3].

Differences in the functional purposes of these actors determine the specific nature of their management needs. For some actors, the identification of military threats, operational planning and command and control are of primary importance; for others, the principal priorities include state border protection, counterterrorism, public security, civil protection, intelligence or counterintelligence activities [12]. Nevertheless, all of them require timely information, threat forecasting, coordinated action and the proper substantiation of management decisions.

Within this study, the management capacity of Ukraine's security and defence forces is proposed to be understood as the comprehensive ability of the relevant authorities, military formations and other actors within the security and defence sector to exercise their statutory powers through the timely acquisition and analysis of information, risk assessment, threat forecasting, activity planning, coordination, and the adoption and implementation of management decisions. This definition represents the authors' interpretation developed within the present

study. Management capacity encompasses not only the availability of resources to the relevant actors but also their functional ability to transform information into specific management decisions and practical actions.

Based on the proposed definition, the following interrelated components should be distinguished within the structure of the management capacity of security and defence forces:

1. Institutional capacity – the existence of clearly defined powers, an appropriate organisational structure and mechanisms of interaction among the relevant actors.

2. Information and analytical capacity – the ability to collect, verify, systematise, process and analyse information obtained from various sources.

3. Forecasting capacity – the ability to identify trends, assess risks and forecast possible developments in the security and operational environment.

4. Planning capacity – the ability to define objectives, develop courses of action, allocate forces, assets and resources, and adjust plans in response to changes in the operational environment.

5. Coordination capacity – the ability to ensure the coherence of actions undertaken by different components of the security and defence sector, facilitate information exchange and support the joint performance of tasks.

6. Capacity for decision-making and implementation – the ability to select a substantiated course of action in a timely manner, communicate decisions to those responsible for their execution, organise their implementation and monitor the results.

7. Adaptive capacity – the ability to modify structures, procedures, tactics and management approaches in response to emerging threats, new technologies and acquired practical experience/

The proposed components do not function in isolation. The quality of a management decision depends on the completeness of the available information;

forecasting results influence planning, while the implementation of plans requires coordination and control. Therefore, management capacity should be regarded as an integrated system in which the weakening of one component may reduce the effectiveness of the entire management process [14].

Artificial intelligence affects management capacity primarily by

expanding the possibilities for working with information [7]. Algorithmic systems can process large volumes of structured and unstructured data, identify hidden relationships, compare information obtained from various sources, and present analytical results in a form suitable for use by public officials and military command authorities.

MANAGEMENT CYCLE USING ARTIFICIAL INTELLIGENCE

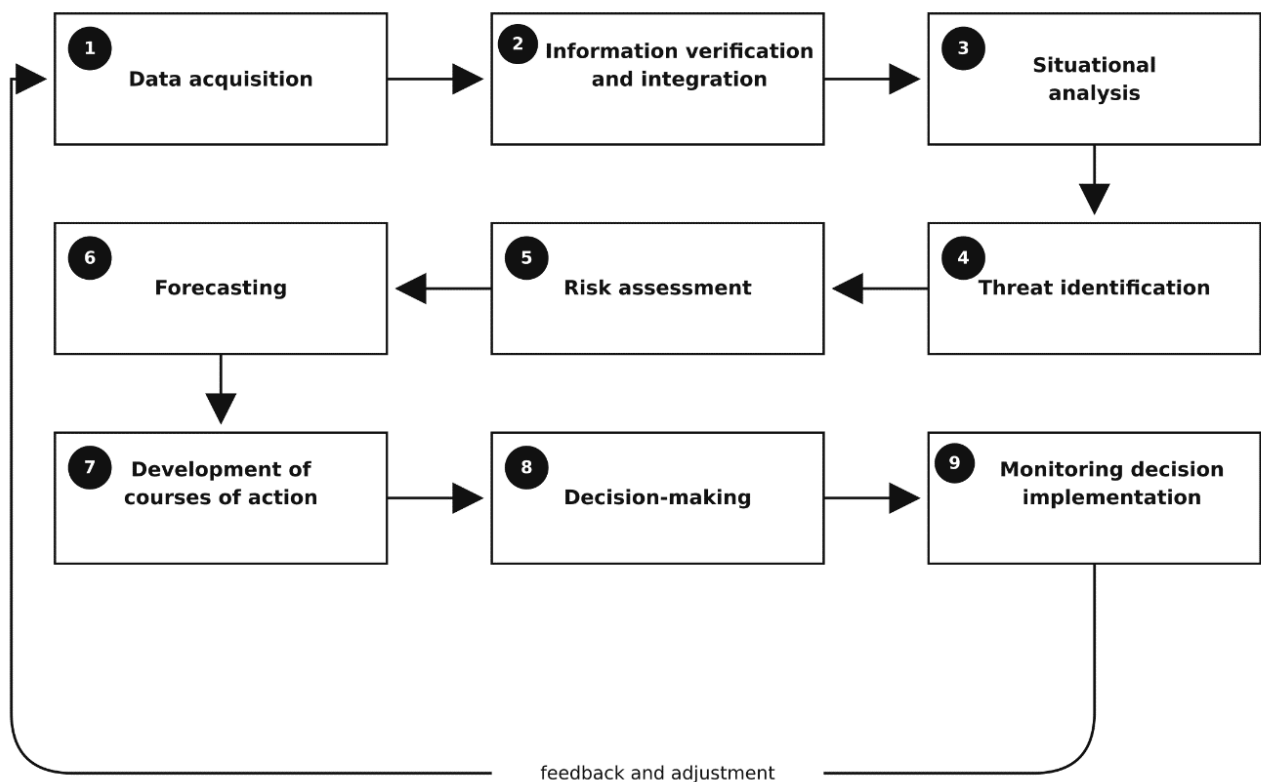


Figure 1. Management cycle using artificial intelligence
Source: Developed by the authors based on their own research.

At each of these stages, artificial intelligence can perform a supporting function by filtering information, detecting anomalies, forecasting possible developments, comparing alternative scenarios and identifying deviations during decision implementation. As a result, the time between receiving information and initiating a management response is reduced, situational awareness is enhanced, and conditions are created for a more

substantiated allocation of forces and resources.

Therefore, AI should be regarded not as an autonomous management actor but as an information, analytical and forecasting tool supporting the activities of authorised actors. It can prepare data, identify relationships, propose courses of action and forecast their possible consequences. However, the final decision and responsibility for it must remain with the competent official.

These steps do not involve replacing a human manager with an algorithmic system. Instead, they provide for the development of a human-machine interaction model in which the technological capabilities of AI are combined with professional experience, contextual understanding, critical thinking and human legal responsibility [11]. Only under these conditions can the use of artificial intelligence genuinely enhance, rather than merely complicate, the management capacity of Ukraine's security and defence forces [8]

Further examination of the role of artificial intelligence requires the systematisation of its functions in the

activities of Ukraine's security and defence forces. In this context, AI functions should be defined not according to the technical characteristics of algorithmic systems but according to their influence on the content, speed and effectiveness of management processes [6].

Based on the conducted research, it is proposed to distinguish the information and analytical, monitoring, forecasting, planning, coordination, resource optimisation and control functions of artificial intelligence, as well as its decision-support function, in the activities of Ukraine's security and defence forces (Table 1).

Table 1. Management functions of artificial intelligence in the activities of Ukraine's security and defence forces

Management function	Content of AI application	Impact on management capacity
Information and analytical	Collection, systematisation, processing and comparison of structured and unstructured data obtained from different sources	Increasing the completeness and speed of information processing; reducing the workload on analytical units
Monitoring	Continuous monitoring of changes in the security and operational environment, detection of anomalies and deviations from specified parameters	Improving situational awareness and ensuring the timely detection of changes in the operational environment
Forecasting	Identification of trends, assessment of the probability of threats and modelling of possible scenarios	Increasing the validity of forecasts and enabling preventive management responses
Planning	Development and comparison of alternative courses of action, modelling of their potential consequences and adjustment of plans	Improving the quality of strategic, operational and tactical planning
Coordination	Integration of information from different agencies, support for information exchange and coordination of joint actions	Strengthening interagency cooperation and reducing delays in transmitting management information
Resource optimisation	Analysis of resource requirements, logistical flows, technical conditions and possible options for allocating forces and assets	Improving the efficiency of the use of personnel, material, technical, financial and time resources
Decision support	Preparation of analytical conclusions, prioritisation of threats and development of alternative courses of action	Reducing the time required to prepare decisions and improving their informational validity

Control	Monitoring the implementation of decisions, comparison of actual results with established objectives and identification of deviations	Ensuring feedback, timely adjustment of actions and increasing executive discipline
---------	---	---

Source: Developed by the authors based on their own research

The proposed systematisation demonstrates that artificial intelligence can be applied at all major stages of the management process. At the same time, the content of each function is determined by the competence of the relevant actor, the nature of its assigned tasks, the level of management and the conditions of the operational environment.

The information and analytical function consists in expanding the capacity of security and defence forces to work with large volumes of heterogeneous information. Such data may include text messages, intelligence data, geospatial information, photographic and video materials, information obtained from technical surveillance systems, data concerning the availability and condition of resources, and other information required for situational assessment [4]. The application of AI makes it possible to accelerate the systematisation of these data, identify recurring patterns and develop a comprehensive information picture.

The monitoring function involves continuously monitoring changes in the security and operational environment. Algorithmic systems can detect anomalous events, atypical changes in indicators, potential signs of emerging threats or deviations from established parameters [5]. This entails shifting the emphasis from responding to events that have already occurred to their timely identification and prevention.

The forecasting function involves using accumulated data to identify trends and model possible developments. AI can assist in assessing the probability of specific threats, forecasting changes in the operational environment, determining the possible consequences of adopted decisions and

identifying factors that may affect the achievement of established objectives [2]. At the same time, algorithmic forecasts should not be regarded as indisputably reliable predictions but as one of the informational elements used in preparing management decisions.

The planning function consists in using AI to develop, model and compare possible courses of action. Algorithmic systems can assist in assessing resource requirements, time constraints, potential risks and the expected outcomes of each scenario. This contributes to improving the validity of strategic, operational and tactical planning but does not eliminate the need for the professional assessment of proposed options by authorised officials.

The coordination function is reflected in ensuring the coherence of actions undertaken by different actors within the security and defence sector. Artificial intelligence can facilitate the integration of information received from different authorities and units, detect inconsistencies in data, identify shared priorities and promptly communicate the necessary information to the relevant actors [13]. However, the implementation of this function depends on the interoperability of information systems, the availability of common data standards and a legally established procedure for interagency information exchange.

The resource optimisation function encompasses the analysis of requirements for forces, assets, material and technical resources, transport, communications, medical support and other components of security and defence activities. Algorithmic systems can contribute to forecasting requirements, identifying critical shortages,

optimising logistics routes, monitoring the technical condition of equipment and ensuring a more rational allocation of available resources.

The management decision-support function is integrative because it combines the results of the information and analytical, monitoring, forecasting and planning functions. AI can synthesise information, prioritise threats, compare alternative courses of action and forecast their possible consequences. Nevertheless, an algorithmic recommendation should not automatically become a management decision. It must be verified with due regard to the operational context, the reliability of source data, legal restrictions and potential consequences.

The control function is implemented by comparing actual results with the established objectives, indicators and parameters of decision implementation. Algorithmic systems can promptly identify deviations, determine factors hindering task performance and provide information on the need to adjust existing plans. This ensures feedback between an adopted decision, the process of its implementation and subsequent management responses.

The management potential of artificial intelligence lies not in performing a single isolated function but in combining different capabilities within an integrated management cycle. Information obtained through monitoring is used for analysis and forecasting; forecasting results provide the basis for planning; developed courses of action are used in decision-making; and monitoring decision implementation generates new data for further analysis and activity adjustment.

At the same time, the introduction of artificial intelligence does not imply the complete transfer of the relevant functions to algorithmic systems. Rather, it involves the technological enhancement of management activities, whereby AI supports information processing, modelling and the preparation of recommendations, while goal setting, the

assessment of legal and societal consequences, the selection of the final course of action and responsibility for its implementation remain with humans [1].

Conclusions.

The conducted research demonstrates that artificial intelligence should be considered not only as a technological innovation but also as an important tool for enhancing the management capacity of Ukraine's security and defence forces. Under conditions of increased risk, time constraints, incomplete information, adversarial interference and rapidly changing operational environments, AI technologies can improve the speed of data processing, situational awareness, threat forecasting, activity planning, interagency coordination and the informational validity of management decisions.

The management capacity of Ukraine's security and defence forces is defined as the comprehensive ability of the relevant authorities, military formations and other actors within the security and defence sector to exercise their statutory powers through the timely acquisition and analysis of information, risk assessment, threat forecasting, activity planning, coordination, and the adoption and implementation of management decisions. This capacity includes institutional, information and analytical, forecasting, planning, coordination and adaptive components, as well as the capacity to adopt and implement decisions. These components form an integrated system in which the effectiveness of each element influences the overall quality of management.

The study establishes that artificial intelligence can support all stages of the management cycle: data acquisition, information verification and integration, situational analysis, threat identification, risk assessment, forecasting, the development of courses of action, decision-making and monitoring of decision implementation. The use of AI can reduce the time between receiving information and initiating a



management response, identify patterns and anomalies in large datasets, compare alternative courses of action and facilitate the rational allocation of forces and resources.

The principal management functions of artificial intelligence in the activities of Ukraine's security and defence forces have been systematised. They include information and analytical, monitoring, forecasting, planning, coordination, resource optimisation and control functions, as well as the decision-support function. The management potential of AI lies not in the isolated performance of individual operations but in integrating these functions within a continuous management cycle supported by feedback and the adjustment of actions.

At the same time, the implementation of artificial intelligence should not result in the transfer of management authority to algorithmic systems. AI should be regarded as an information, analytical and forecasting tool that assists authorised actors in preparing and implementing decisions. Algorithmic recommendations require professional assessment based on the operational context, the reliability and completeness of source data, legal restrictions, potential risks and the possible consequences of the proposed actions.

Effective AI application requires the development of a human-machine interaction model in which technological capabilities are combined with professional experience, critical thinking and contextual understanding. Goal setting, assessment of legal and societal consequences, selection of the final course of action and responsibility for its implementation must remain with the competent official. Preserving meaningful human oversight is therefore a fundamental condition for the responsible use of artificial intelligence by security and defence forces.

Further research should focus on developing criteria and indicators for assessing the impact of AI on management capacity, identifying the specific features of its application by different actors within Ukraine's security and defence sector, improving interagency data exchange and information-system interoperability, and establishing organisational safeguards for human oversight and accountability. Addressing these issues will facilitate the responsible integration of AI into management processes and strengthen the adaptability, resilience and effectiveness of Ukraine's security and defence forces.

References

1. Alon-Barkat, S., & Busuioc, M. (2023). Human-AI interactions in public sector decision making: "Automation bias" and "selective adherence" to algorithmic advice. *Journal of Public Administration Research and Theory*, 33(1), 153–169. <https://doi.org/10.1093/jopart/muac007> [in English].
2. Alon-Barkat, S., & Busuioc, M. (2024). Public administration meets artificial intelligence: Towards a meaningful behavioral research agenda on algorithmic decision-making in government. *Journal of Behavioral Public Administration*, 7. <https://doi.org/10.30636/jbpa.71.261> [in English].
3. Verkhovna Rada of Ukraine. (2018). On the National Security of Ukraine: Law of Ukraine No. 2469-VIII of June 21, 2018. *Vidomosti Verkhovnoi Rady Ukrainy*, 31, Art. 241. <https://zakon.rada.gov.ua/laws/show/2469-19#Text> [in Ukrainian].



4. Harmash, O. M., Fedorenko, T. V., & Hvozdoва, O. O. (2026). Corporate cyber risk governance as a factor in the economic security of defence-industrial enterprises. *Actual Problems of Innovative Economy and Law*, 3, 57–64. <https://doi.org/10.36887/2524-0455-2026-3-9> [in Ukrainian].
5. Ilin, A. O. (2025). Artificial intelligence in public authorities as a pathway to the formation of innovative institutions. *Scientific Perspectives*, 2(56), 823–847. [https://doi.org/10.52058/2708-7530-2025-2\(56\)-823-847](https://doi.org/10.52058/2708-7530-2025-2(56)-823-847) [in Ukrainian].
6. Karpenko, O. V., & Karpenko, Yu. V. (2021). Artificial intelligence as a tool for public administration of socio-economic development: Smart infrastructure, digital business analytics systems and transfers. *Public Administration: Improvement and Development*, 10. URL: <http://www.dy.nayka.com.ua/?op=1&z=2257> [in Ukrainian].
7. Kyrych, N. (2024). The influence of digitalization on modern management processes. In *Business Transformation for a Sustainable Future: Research, Digitalization and Innovation: A Monograph* (pp. 363–372). Ternopil: Ternopil Ivan Puluj National Technical University. URL: <https://elartu.tntu.edu.ua/handle/lib/46660> [in Ukrainian].
8. Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020). Military applications of artificial intelligence: Ethical concerns in an uncertain world. RAND Corporation. <https://doi.org/10.7249/RR3139-1> [in English].
9. Nikoliuk, O. V., Rodina, O. V., & Savchenko, T. V. (2023). Problems and advantages of artificial intelligence as an effective institution for the development of management solutions in public administration. *Scientific Notes of V. I. Vernadsky Taurida National University. Series: Public Administration and Management*, 34(73), 3, 124–130. URL: <https://surl.li/pjenta> [in Ukrainian].
10. Sporyshev, K. (2024). Analysis of the regulatory framework for information and analytical support of the security forces of Ukraine: aspects of public administration. *Honor and Law*, (1 (88), 142–149. <https://doi.org/10.33405/2078-7480/2024/1/88/302293>
11. Pshenychna, T. V. (2024). Integration of artificial intelligence technologies into public administration at the local level: New horizons and challenges. *Efficiency of Public Administration*, 3(80/81), 94–104. <https://doi.org/10.36930/508013> [in Ukrainian].
12. Pustovit, Ya. B. (2026). State policy on the use of artificial intelligence technologies in the defence sector of Ukraine. *Actual Problems of Innovative Economy and Law*, 3, 191–195. <https://doi.org/10.36887/2524-0455-2026-3-36> [in Ukrainian].
13. Sposato, M., & Dittmar, E. C. (2026). The AI-powered future of digital transformation: Enhancing organizations and leadership development. *Journal of Work-Applied Management*. <https://doi.org/10.1108/JWAM-02-2025-0039> [in English].
14. Zakhmi, K. (2023). AI and integrity: Balancing innovation with ethical responsibility beyond the algorithm. *Journal of Artificial Intelligence, Machine Learning and Data Science*, 3(2), 2. URL: <https://urfjournals.org/open-access/ai-and-integrity-balancing-innovation-with-ethical-responsibilitybeyond-the-algorithm.pdf> [in English].