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

ISSN 2708-3195
9772708319005

Electronic scientific and practical collection
INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT

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;
HLYNSKYY 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

facebook.com/Smart.SCM.org
DOI: https://doi.org/10.46783/smart-scm/2026-38
тел.: (063) 593-30-41
e-mail: support@smart-scm.org
https://smart-scm.org

Contents

INTRODUCTION 7

HRYHORAK 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

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

111-121
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-8

UDC 351.746.1
JEL Classification: F52, H56, O33.

Received: 2026-07-21
Accepted: 2026-08-26
Published: 2026-08-30

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

ORCID – 0000-0001-8549-2910
Researcher ID HKO-6132-2023
Scopus author id: – 57148526900
E-Mail: sorokivska_o@tntu.edu.ua

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

Olena Sorokivska "International information security in the context of the emergence of a global information society" *This article examines the theoretical and methodological foundations for ensuring international information security in the context of the emerging global information society. It is argued that the rapid development of digital technologies, the globalization of information flows, and the spread of artificial intelligence, big data, cloud computing, digital platforms, and cross-border communications are significantly transforming the international security environment, creating not only new opportunities for the development of states and societies but also a wide range of information risks and threats. It is determined that the information space is increasingly becoming an independent sphere of international confrontation, where, alongside traditional instruments, information and psychological operations, cyberattacks, digital espionage, manipulation of public opinion, disinformation, and other forms of hybrid influence are employed. This paper analyzes current trends in the development of the global information society and their impact on the transformation of international information security. It examines the activities of international organizations and integration associations aimed at establishing mechanisms for international cooperation in the field of information security, developing global digital security standards, and countering cybercrime, information operations, and transnational information threats. This paper identifies the key factors influencing the state of international information security in the context of the global information society. It substantiates conceptual directions for improving the international information security system, including: the development of international digital diplomacy; the creation of integrated mechanisms for monitoring information threats; improving strategic communications systems; implementing intelligent technologies for analyzing the information space; developing international information exchange regarding cyber incidents; establishing uniform standards for digital trust and information resilience; and strengthening partnerships among states, international organizations, research institutions, and the private sector in the field of protecting the global information space.*

Keywords: information security, globalization, information society, threats, national security, cyberspace, international cooperation, digital technologies

Олена Сороківська «Міжнародна інформаційна безпека в контексті формування глобального інформаційного суспільства». *У статті досліджено теоретико-методологічні*

This work is licensed under a Creative Commons Attribution 4.0 International License

111-121
v.38 (2026)
https://smart-scm.org

засади забезпечення міжнародної інформаційної безпеки в умовах формування глобального інформаційного суспільства. Обґрунтовано, що стрімкий розвиток цифрових технологій, глобалізація інформаційних потоків, поширення штучного інтелекту, великих даних, хмарних обчислень, цифрових платформ і транскордонних комунікацій суттєво трансформують міжнародне безпекове середовище, створюючи не лише нові можливості для розвитку держав і суспільств, а й широкий спектр інформаційних ризиків та загроз. Визначено, що інформаційний простір дедалі більше перетворюється на самостійну сферу міжнародного протиборства, де поряд із традиційними інструментами використовуються інформаційно-психологічні операції, кібератаки, цифрове шпигунство, маніпулювання громадською думкою, дезінформація та інші форми гібридного впливу. Проаналізовано сучасні тенденції розвитку глобального інформаційного суспільства та їх вплив на трансформацію міжнародної інформаційної безпеки. Досліджено діяльність міжнародних організацій та інтеграційних об'єднань щодо формування механізмів міжнародного співробітництва у сфері інформаційної безпеки, розвитку глобальних стандартів цифрової безпеки, протидії кіберзлочинності, інформаційним операціям і транснаціональним інформаційним загрозам. У роботі визначено основні чинники, що впливають на стан міжнародної інформаційної безпеки в умовах глобального інформаційного суспільства. Обґрунтовано концептуальні напрями вдосконалення системи міжнародної інформаційної безпеки, серед яких: розвиток міжнародної цифрової дипломатії; створення інтегрованих механізмів моніторингу інформаційних загроз; удосконалення систем стратегічних комунікацій; впровадження інтелектуальних технологій аналізу інформаційного простору; розвиток міжнародного обміну інформацією щодо кіберінцидентів; формування єдиних стандартів цифрової довіри та інформаційної стійкості; зміцнення партнерства між державами, міжнародними організаціями, науковими установами й приватним сектором у сфері захисту глобального інформаційного простору.

Ключові слова: інформаційна безпека, глобалізація, інформаційне суспільство, загрози, національна безпека, інформаційний простір, міжнародне співробітництво, цифрові технології..

Introduction. The emergence of a global information society is one of the defining trends in contemporary global development, accompanied by the rapid spread of digital technologies, an increase in the volume of information exchange, and growing interdependence among nations. The digitization of international relations opens up new opportunities for economic development, international cooperation, and innovative governance, while simultaneously creating new challenges in the field of international information security. Threats related to cyberattacks, disinformation, information and psychological operations, interference in the internal affairs of states through the information space, and the use of digital technologies as a tool of geopolitical influence are of particular concern. In today's world, the information space is increasingly becoming a distinct dimension of international competition, where information serves as both a strategic resource and an object requiring protection. The transnational nature of information threats significantly complicates individual states' ability to detect and neutralize them in a timely manner. This necessitates strengthening international cooperation, developing mechanisms for collective response, and improving international legal regulation in the field of information security. At the same time, the rapid pace of development in digital technologies is far outpacing the adaptation of existing international institutional and legal mechanisms, which reduces the effectiveness of efforts to counter modern information threats. Under these conditions,

This work is licensed under a Creative Commons Attribution 4.0 International License

the search for new conceptual approaches to ensuring international information security—based on the principles of international partnership, digital resilience, and information trust—becomes particularly relevant. Research into current trends in the development of international information security in the context of the formation of a global information society is an important prerequisite for improving international policy in the field of protecting the global information space and ensuring the sustainable development of the global community.

Analysis of recent research and publications. Issues related to international information security, the development of the global information society, digital transformation, and countering modern information threats are the focus of the domestic scientific community. Research by Ukrainian scholars covers the legal, managerial, institutional, technological, and international-political aspects of ensuring information security, which attests to the interdisciplinary nature of this field.

The scholarly works of O. A. Baranov, V. G. Pylypchuk, and I. M. Doronin are devoted to the development of the theoretical and legal foundations of information security, the improvement of information legislation, the formulation of state policy in the field of cybersecurity and information law, as well as the harmonization of the national information protection system with European and international standards. The researchers pay particular attention to issues related to the legal framework for digital transformation, combating cybercrime, and developing mechanisms to protect Ukraine's information space.

The research by O. P. Dzoban, I. V. Aristova, and K. I. Belyakov focuses on issues of public administration in the field of information security, the development of state information policy, the functioning of mechanisms for ensuring information security in government agencies, and the improvement of the organizational and legal framework for state regulation in the context of digitalization. The authors' works justify the need to integrate modern digital technologies, international experience, and European approaches into the development of the information security system.

At the same time, issues related to ensuring international information security—specifically in the context of the formation of a global information society, the development of international digital diplomacy, the improvement of international coordination mechanisms, countering cross-border information threats, and the establishment of unified international standards for digital trust—remain insufficiently studied in a comprehensive manner. This necessitates further scholarly examination of the conceptual foundations for the development of international information security, taking into account contemporary processes of digital transformation, the globalization of the information space, and the growing role of international cooperation in countering the latest information challenges.

The formulation of the goals of the article to study the theoretical foundations of international information security in the context of the emergence of a global information society, to identify contemporary information threats, and to justify priority areas for improving international mechanisms for ensuring information security.

Presentation of the main results. The emergence of a global information society is a natural consequence of the development of digital technologies, international integration, and the intensive exchange of information, which is fundamentally transforming contemporary social and international processes. Under these conditions, ensuring international information security has become one of the top priorities of international policy, as the resilience of the global information space

This work is licensed under a Creative Commons Attribution 4.0 International License

directly affects the stability of states, international institutions, and the global security system.

The rapid development of digital technologies is fundamentally changing the modern system of international relations, contributing to the formation of a global information society in which information and digital data are becoming strategic resources. The globalization of information flows enables an unprecedented speed of cross-border information exchange and expands opportunities for international cooperation, economic integration, e-governance, and the development of the digital economy. At the same time, the widespread adoption of artificial intelligence, big data analytics, cloud computing, and digital platforms significantly enhances the efficiency of management processes, automated decision-making, risk forecasting, and the operation of critical infrastructure. At the same time, digitalization significantly increases the dependence of states, international organizations, and society on information and communications infrastructure, making it a potential target for external influence [1].

The transformation of the international security environment is reflected in the changing nature of contemporary threats, which are increasingly of an informational and cyber nature. The use of digital technologies creates conditions for large-scale cyberattacks, information and psychological operations, the spread of disinformation, the manipulation of public opinion, interference in electoral processes, digital espionage, and disruptions to critical information infrastructure. A particular danger is posed by the use of artificial intelligence for the automated creation of disinformation content, deepfake technologies, personalized information campaigns, and the refinement of cyberattack tools. Furthermore, the cross-border nature of digital communications significantly complicates the identification of sources of information attacks, the determination of jurisdiction, and the prosecution of actors engaged in unlawful activities in the global information space [2].

Thus, modern digital technologies serve simultaneously as a powerful driver of social development and a source of new information risks, which necessitates the improvement of international mechanisms for ensuring information security, the development of international cooperation, the harmonization of legal regulations, and the establishment of an effective system for collectively countering global information threats.

It is worth noting that the information space is increasingly becoming a distinct arena of international competition, within which states, international organizations, and non-state actors employ a wide range of instruments of influence; therefore, it is appropriate to classify them into traditional and modern categories [3]:

1. Traditional instruments of international information competition

- diplomatic information influence—the use of official statements, international negotiations, diplomatic channels, and public diplomacy to advance national interests;
- propaganda and counterpropaganda—the systematic dissemination of information aimed at shaping the desired international image of a state or discrediting an opponent;
- informational and psychological influence—the targeted influence on public consciousness and the moral and psychological state of the population, the military, and political elites;
- activities of traditional mass media—the use of television, radio, print media, and international news agencies to shape public opinion;
- political and economic communication—the use of information resources during international negotiations, the implementation of sanctions policies, and the execution of foreign policy strategies.

2. Modern tools of international information warfare:

This work is licensed under a Creative Commons Attribution 4.0 International License

111-121
v.38 (2026)
https://smart-scm.org

- cyberattacks – unauthorized interference with information systems, government information resources, and critical information infrastructure;

- digital espionage – the illegal acquisition of confidential information through the use of cyber tools, malware, and digital data collection channels;

- disinformation and the dissemination of fake content – the deliberate spread of false or manipulative information to achieve political, military, or economic goals;

- manipulation of public opinion through digital platforms – the use of social media, recommendation algorithms, bot networks, targeted advertising, and other digital technologies to influence public sentiment.

- next-generation information and psychological operations—the comprehensive use of digital technologies, social media, artificial intelligence, and big data technologies to exert targeted informational influence;

- artificial intelligence and deepfake technologies—the automated creation of realistic audio, video, and text content for the purpose of disinformation, discrediting, or misleading a target audience;

- hybrid information operations—a combination of cyber tools, information and psychological influence, economic pressure, political instruments, and diplomatic measures within a unified strategy to achieve geopolitical goals.

Thus, modern international information warfare is characterized by the integration of traditional and digital tools of influence. While traditional methods were primarily aimed at shaping international public opinion through classic communication channels, modern technologies enable high-speed, large-scale, personalized, and often covert influence on the information space, which significantly complicates efforts to ensure international information security and requires the development of new mechanisms for international cooperation and collective response.

The emergence of a global information society is accompanied by a large-scale digital transformation of the global landscape, which is changing the nature of international interaction, economic development, public administration, and security processes. Modern digital technologies not only provide new opportunities for the integration of states and the development of international cooperation but also give rise to fundamentally new challenges in the field of international information security. In this regard, it is advisable to analyze the key trends in the development of the global information society and determine their impact on the transformation of the international security environment [4]:

Table 1 – Current trends in the development of the global information society and their impact on the transformation of international information security

Current Trends in the Development of the Global Information Society	Characteristics of the Trend	Impact on International Information Security
The Globalization of the Information Space	The rapid growth of cross-border information flows, digital communications, and international information exchange.	It strengthens the interdependence of nations, but at the same time increases the risks of cross-border cyberattacks, disinformation, and information interference.
Digital Transformation of Public Administration	Active implementation of e-government, digital services, and interagency information sharing.	It improves the efficiency of public administration while highlighting the need to protect government information resources and critical digital infrastructure.

This work is licensed under a Creative Commons Attribution 4.0 International License

111-121
v.38 (2026)
https://smart-scm.org

The Spread of Artificial Intelligence and Big Data Technologies	The use of intelligent algorithms to automate processes, analyze information, and support management decisions.	It expands the capabilities for predicting and monitoring threats, but creates risks related to the automation of cyberattacks, information manipulation, and the use of deepfake technologies
The Dominance of Digital Platforms and Social Media	Digital platforms are becoming the primary medium for international communication and the dissemination of information.	They facilitate the global exchange of information, but they also create the conditions for the widespread dissemination of disinformation, information and psychological operations, and the manipulation of public opinion.
Digitalization of Critical Infrastructure	The integration of digital technologies into the operations of the energy sector, transportation, the financial system, healthcare, and the public sector.	It improves the efficiency of managing critical systems, but also increases their vulnerability to international cyberattacks and cyberterrorism.
Strengthening International Cooperation in the Field of Cybersecurity	The development of international mechanisms for coordination, information exchange, and the harmonization of information security standards.	It lays the groundwork for a collective response to global information threats, strengthens digital resilience, and improves the international information security system.

Source: compiled by the author based on data from [5]

Consequently, current trends in the development of the global information society are significantly transforming the international information environment, altering both the nature of international interaction and the nature of information threats. Digitalization, the development of artificial intelligence, global digital platforms, cloud technologies, and cross-border information communications are creating new opportunities for the sustainable development of states, but at the same time are increasing the vulnerability of the international information space to cyber threats, disinformation, and hybrid influences. Under these conditions, international information security takes on a multifaceted character, necessitating the improvement of international legal mechanisms, the development of interstate coordination, the strengthening of digital resilience, and the establishment of an effective system for collective response to contemporary information threats.

Current trends in the development of the global information society indicate that information threats are increasingly taking on a cross-border nature, extending beyond the jurisdiction of individual states and posing risks to international security. Under these conditions, effectively ensuring international information security can no longer rely solely on national mechanisms but requires the consolidation of the international community's efforts, the harmonization of regulatory and legal approaches, and the development of institutional mechanisms for international cooperation. In this regard, the activities of international organizations and integration associations take on particular significance, as they shape the modern architecture of international information security, develop global digital security standards, and coordinate joint measures to counter cybercrime, information operations, and transnational information threats [6-8]:

1) The United Nations (UN)—establishing international legal principles for responsible state behavior in cyberspace and fostering global dialogue on information security. The work of the UN Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG); the development of voluntary norms for responsible state behavior in cyberspace; and the promotion of

This work is licensed under a Creative Commons Attribution 4.0 International License

international cooperation in the field of cybersecurity.

2) NATO—integration of cybersecurity and information security into the collective defense system; development of member states' cyber resilience. Recognition of cyberspace as a distinct operational domain; activities of the Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn; conduct of the international exercises Locked Shields and Cyber Coalition; exchange of information on cyber threats.

3) European Union (EU) – harmonization of digital legislation; enhancing the cyber resilience of member states; protecting the digital market and critical infrastructure. Adoption of the NIS2 Directive, the DORA Regulation, the Cybersecurity Act, and the Cyber Solidarity Act; activities of ENISA; creation of a CSIRT network for rapid response to cyber incidents.

4) Council of Europe – combating cybercrime and improving international cooperation in criminal law. The Convention on Cybercrime (Budapest Convention) and the Second Additional Protocol on Electronic Evidence; international cooperation among law enforcement agencies during cybercrime investigations.

5) Organization for Security and Cooperation in Europe (OSCE) – reducing the risks of conflict in the digital environment and building trust among states regarding the use of ICT. Implementation of Confidence-Building Measures (CBMs) in cyberspace; consultations among states on the prevention of cyber incidents; mechanisms for transparency and information sharing.

6) International Telecommunication Union (ITU) – development of global digital infrastructure and international standards for information and communication technologies. Global Cybersecurity Agenda (GCA); Global Cybersecurity Index (GCI); development of international technical standards and support for the development of states' cybersecurity capabilities.

7) International Criminal Police Organization (INTERPOL) — coordination of the international fight against cybercrime and transnational digital crimes. The work of the Cybercrime Directorate; international operations against ransomware, botnets, and online fraud; and the operations of the Global Complex for Innovation in Singapore.

An analysis of the activities of international organizations shows that the modern system of international information security is based on multilevel cooperation, within which each institution performs specialized functions. The UN defines general principles of international law governing states' conduct in cyberspace; NATO ensures the development of collective cyber defense and cyber resilience; the European Union establishes a comprehensive regulatory framework for digital security; the Council of Europe coordinates international efforts to combat cybercrime, the OSCE develops confidence-building mechanisms in cyberspace, the ITU establishes global technical standards, and Interpol facilitates international cooperation among law enforcement agencies in the fight against transnational cybercrime.

This comprehensive approach demonstrates that ensuring international information security can no longer be achieved solely at the national level, but requires constant coordination among states, international organizations, the scientific community, and the private sector, as well as the harmonization of international legal, organizational, and technological mechanisms for responding to modern information threats.

However, despite the active development of international cooperation in the field of information security and the improvement of international legal mechanisms to counter modern threats, the global information environment continues to undergo dynamic transformation under the influence of technological, political, and social processes. This gives rise to new factors that

This work is licensed under a Creative Commons Attribution 4.0 International License

111-121
v.38 (2026)
https://smart-scm.org

shape the current state of international information security, alter the nature of information confrontation, and require constant updating of approaches to ensuring the resilience of the global information space (Table 2).

Table 2 – Key factors influencing the state of international information security in the context of the global information society

Factor	Manifestations in the Current Context
1. The digital transformation of society	The widespread digitization of public administration, the economy, education, the financial system, and critical infrastructure improves the efficiency of societal processes, but at the same time increases the number of potential targets for cyberattacks and unauthorized access to information.
2. The development of artificial intelligence	The use of AI for information analysis, the automation of management processes, cybersecurity, and risk forecasting is accompanied by the potential for its use in the automated creation of disinformation, cyberattacks, personalized information influence, and deepfake technologies.
3. The intensification of information wars and hybrid conflicts	The information space is used as a separate arena of international confrontation, where information and psychological operations are combined with military, political, economic, and cyber instruments of influence.
4. The spread of cyberterrorism and transnational cybercrime	There has been an increase in the number of attacks on government agencies, critical infrastructure, financial institutions, the energy sector, and international information networks using ransomware, malware, and other cyber tools.
5. The use of deepfake technologies and the automation of information and psychological influence	Realistically generated audio, video, and text content, automated bot networks, and generative AI algorithms are being used to manipulate public opinion, discredit political leaders, and destabilize the information environment.
6. The use of algorithmic systems and digital interdependence among nations	The algorithms of digital platforms determine the dissemination of information and shape the information agenda, while the high level of integration of digital infrastructures and global services leads to the rapid spread of information threats across nations and heightens the need for international coordination.

Source: compiled by the author based on data from [9-10]

Thus, the current state of international information security is determined by a complex of interrelated technological, political, and security factors that are significantly transforming the nature of the global information environment. Digital transformation, the development of artificial intelligence, the intensification of information warfare, cyberterrorism, deepfake technologies, the automation of information and psychological influence, the algorithmization of digital platforms, and the growing digital interdependence of states are shaping a new architecture of international information security. This indicates that modern information threats are complex and transnational in nature, and their effective prevention is possible only through a combination of technological innovations, international legal regulation, interstate coordination, and the development of mechanisms for collectively ensuring information resilience.

An analysis of current trends in the development of the global information society and the key factors influencing international information security shows that modern information threats are complex and transnational in nature, as their emergence, spread, and consequences are not limited by national borders. The rapid development of digital technologies, the global integration of information systems, and the high level of digital interdependence among states

This work is licensed under a Creative Commons Attribution 4.0 International License

contribute to the rapid spread of cyber threats, disinformation, information and psychological operations, and other forms of hybrid influence, which can simultaneously affect multiple countries and regions.

Under these circumstances, effectively preventing and countering cyberattacks, information and psychological operations, disinformation, digital espionage, cyberterrorism, manipulation of public opinion, the use of deepfake technologies, and other forms of hybrid information influence requires a systematic international approach based on the coordination of efforts by states, international organizations, the private sector, and the scientific community; the harmonization of international legal norms; the development of mechanisms for the rapid exchange of information; a coordinated response to cyber incidents; and the strengthening of global digital resilience.

At the same time, the deepening digital transformation of the global community, the growing number of cross-border information threats, and the insufficient effectiveness of existing international response mechanisms necessitate the improvement of the international information security system. Under current conditions, its development must be based on a comprehensive combination of legal, organizational, technological, and institutional mechanisms aimed at ensuring the resilience of the global information space. In this regard, it is appropriate to identify the following conceptual directions for improving international information security [11]:

1) Development of international digital diplomacy—this involves expanding international dialogue to develop common approaches to regulating the digital space, coordinating information security policies, and preventing international information conflicts;

2) Creating integrated mechanisms for monitoring information threats—establishing international platforms for the early detection of information threats will ensure the timely exchange of analytical data, risk forecasting, and the coordination of joint actions to mitigate them;

3) Improving strategic communications systems—developing international cooperation in the field of strategic communications will help increase the effectiveness of countering disinformation, information and psychological operations, and other forms of hybrid influence;

4) Implementation of intelligent technologies for analyzing the information space—the use of artificial intelligence, Big Data, and machine learning will enable the automation of detecting information attacks, analyzing trends in the spread of disinformation, and forecasting potential threats;

5) Developing international information sharing on cyber incidents—establishing effective mechanisms for the rapid exchange of information among states, international organizations, and national response centers will facilitate the swift containment of cyber incidents and minimize their consequences;

6) establishing uniform standards for digital trust and information resilience—the harmonization of international regulatory, legal, and technical standards will help enhance the security of digital infrastructure, foster the development of a secure digital environment, and strengthen trust among participants in international cooperation;

7) Strengthening partnerships among states, international organizations, research institutions, and the private sector—consolidating the resources and expertise of all stakeholders will ensure a comprehensive approach to developing innovative solutions, training specialists, conducting joint research, and establishing an effective international information security system.

Thus, improving the international information security system requires a shift from a predominantly reactive response to information threats to a proactive model of international governance based on risk forecasting, international coordination, and

This work is licensed under a Creative Commons Attribution 4.0 International License

the widespread use of digital innovations. The priority areas for such development include strengthening international digital diplomacy, implementing smart technologies for monitoring and analyzing the information space, improving strategic communications systems, harmonizing international digital security standards, and deepening partnerships among states, international organizations, the scientific community, and the private sector. Implementing these priorities will contribute to the development of a resilient, adaptive, and effective international information security system capable of ensuring an adequate level of protection for the global information space amid ongoing digital transformation and the rise of transnational information threats.

Conclusions.

Thus, the emergence of a global information society is fundamentally transforming the international security environment, turning the information space into one of the key dimensions of international interaction and confrontation. The rapid development of digital technologies, the spread of artificial intelligence, the globalization of information flows, and the growth of digital interdependence among states—along with new opportunities—are giving rise to a complex set of transnational information threats that cannot be effectively countered at the national level alone. This study has confirmed the decisive role of international organizations in shaping the modern architecture of international information security, while also demonstrating the need for further improvement of mechanisms for international cooperation. Under current conditions, the development of international digital diplomacy, the harmonization of international digital security standards, the implementation of intelligent technologies for monitoring the information space, the improvement of strategic communications, and the strengthening of partnerships among states, international organizations, the scientific community, and the private sector have become priorities. Implementing these priorities will contribute to the formation of an effective, adaptive, and resilient system of international information security capable of ensuring the protection of the global information space in the face of contemporary civilizational challenges.

References

1. Pylypchuk, V. H., Baranov, O. A., Hyliaka, O. S. (2022). The problem of legal regulation in the field of artificial intelligence in the context of the development of European Union legislation. Bulletin of the National Academy of Legal Sciences of Ukraine. Available at: https://visnyk.kh.ua/uk/author/oleksandr-andriyovich-baranov.

2. Pylypchuk, V. H., Doronin, I. M. (2018). National security law and military law: theoretical and applied foundations of formation and development in Ukraine. Information and Law, Vol. 2(25), pp. 62–72. Available at: https://ippi.org.ua/pilipchuk-vg-doronin-im-pravo-natsionalnoi-bezpeki-ta-viiskove-pravo-teoretichni-ta-prikladni-zasadi.

3. Aristova, I. V., Baranov, O. A., Dzoban, O. P., et al.; Bieliakov, K. I. (Ed.). (2019). Legal liability for offenses in the information sphere and the foundations of information delictology. Kyiv: KVITs. 344 p.

This work is licensed under a Creative Commons Attribution 4.0 International License

4. Bieliakov, K. I. (2018). Legislation in the information security sector: technological and legal analysis. In: Current Issues of Information Security Management of the State: Proceedings of the IX All-Ukrainian Scientific and Practical Conference. Kyiv, pp. 15–19.

5. Kohut, Yu. I. (2024). A new type of hybrid warfare as a threat to national security of the state. Kyiv: DAKOR Publishing House. 348 p.

6. Pavlov, D. M., Mykytiuk, M. A. (2020). Legal and organizational principles of critical infrastructure protection in the context of the formation of Ukraine's new security paradigm. Chest i Zakon, Vol. 4(75), pp. 69–77.

7. Bezverkhniuk, T. M. (2024). Strategic communications for ensuring the synchronization of programs and projects of Ukraine's post-war recovery plan. Public Administration and Administration in Ukraine, Vol. 39, pp. 57–63. Available at: https://pagjournal.iei.od.ua/39-2024.

8. Makovetska, I. M., Yuhov, V. Yu. (2021). Communication management in enterprises. Economics. Management. Business, Vol. 2(36). pp. 32-36. Available at: https://doi.org/10.31673/2415-8089.2021.023338.

9. Onyshchenko, O. V. (2026). Information security as a component of the international system of counter-terrorism. Scientific Bulletin of Uzhhorod National University. Series: Law, Issue 93, Part 5. DOI: https://doi.org/10.24144/2307-3322.2026.93.5.52.

10. Dovhan, O. D., Tkachuk, T. Yu. Legal support of state information security as a sub-branch of information law: theoretical discourse. Available at: https://ippi.org.ua/dovganod-tkachuk-tyu-pravove-zabezpechennya-informatsiinoi-bezpeki-derzhavi-yak-pidgaluzinformatsi.

11. Kylymnyk, I. I. (2023). Information society and information security. New challenges and ways to overcome information threats. Scientific Bulletin of Uzhhorod National University. Series: Law, Vol. 2, No. 76. DOI: https://doi.org/10.24144/2307-3322.2022.76.2.8.

This work is licensed under a Creative Commons Attribution 4.0 International License