Multidisciplinary Reviews

MINI-REVIEW
Published Online: May 29, 2026
https://doi.org/10.31893/multirev.2026spe005

The language of public communication in the contemporary media space: Analytics, risks, and threats to information security

Larysa Holoiukh[a] | Iryna Levchuk[a] | Tetiana Masytska[b] | Oksana Pryimachok[b] | Larysa Sadova[c] | Nataliia Iovkhimchuk[d]

[a]Department of the History and Culture of the Ukrainian Language, Lesya Ukrainka Volyn National University, Lutsk, Ukraine.
[b]Department of Ukrainian Language and Linguistic Didactics, Lesya Ukrainka Volyn National University, Lutsk, Ukraine.
[c]Department of Foreign and Ukrainian Philology, Faculty of Digital Educational and Social Technologies, Lutsk National Technical University, Lutsk, Ukraine.
[d]Department of Theory and Methodology of Primary Education, Faculty of Pedagogical Education and Social Work, Lesya Ukrainka Volyn National University, Lutsk, Ukraine.

Abstract This study is relevant because of the rapid transformation of the media space, in which digital platforms have become the main channel of communication while creating new risks for information security. The growing scale of disinformation, algorithmic manipulation, and hybrid information attacks requires a comprehensive scientific analysis of their impact on public consciousness and public administration. The purpose of the study is to investigate the peculiarities of public communication in the modern media space, to identify key risks to information security and to characterize methodological approaches to their assessment. The methodological basis of the study is the content analysis of international statistical sources, bibliometric analysis of scientific publications and classification of the main threats. As a result, social networks in Ukraine play a more significant role in news consumption than in countries with an established media system does, which increases the risks of manipulation. The main groups of threats—technological, information and communication, sociopsychological, political, cybersecurity, and international—are systematized, forming a multilevel set of challenges. It is shown that algorithmic restrictions create information bubbles that increase the polarization of society, whereas hybrid campaigns undermine trust in institutions and the media. The practical significance of this work lies in the possibility of using the results to formulate state strategies to counter disinformation, develop media literacy education programs, and implement digital systems for monitoring information flows. The proposed methodological approaches can be used for further interdisciplinary research and development of tools to ensure the sustainability of the information environment.

Keywords: media space, public communication, media text, Ukrainian media, linguistic means of communication, communicative competence

1. Introduction

The rapid digitization of the communication environment has significantly transformed the mechanisms of the information space in modern society. Over the past decade, digital platforms and social networks have gradually evolved from auxiliary communication channels into key infrastructure for disseminating news, shaping public discourse, and mobilizing public opinion. According to international analytical studies, a significant part of the population receives political, economic, and social information through online platforms, which changes traditional models of media consumption and transforms the mechanisms of shaping the public agenda. Moreover, this transformation is accompanied by the emergence of new risks associated with the spread of disinformation, algorithmic content selection, automated scaling of messages, and the use of digital technologies to organize information influence (Goncharuk-Cholach et al., 2025).

Information functions as a vital strategic asset that shapes political security and economic growth and maintains public confidence in today's society. Digital communication processes have transformed public discourse into a media-based platform that serves as the primary space for public opinion formation and social initiative mobilization and idea dissemination. The fast pace at which information spreads through multiple communication channels creates two major security risks: the dissemination of false information and deceptive technological systems and sophisticated hybrid information assaults that threaten national and public security.

Scientific interest in the problems of information security and public communication has increased significantly over the past decade. Studies point to the increasing role of social media as the main channel for political and social interaction, which is supported by both international analytical reports and academic works on digital transformations of communication processes (Ng et al., 2025; Hulland, 2024; Torres-Salinas, 2024). Scientists also emphasize the need to develop bibliometric and

content analytical methods to study trends in media consumption and information flows (Donthu, 2021; Marzi et al., 2025). In these studies, a combination of quantitative and qualitative approaches is of particular importance, which allows us not only to assess the scale of information dissemination but also to identify its social and psychological effects. Moreover, despite significant progress in the study of the phenomenon of public communication, the issues of harmonizing the standards of analytical approaches, as well as the problem of assessing the impact of algorithmic restrictions and hybrid manipulations on public consciousness, remain unresolved. Many studies describe individual aspects—technological, political, or sociopsychological—but a comprehensive interdisciplinary model for assessing risks and challenges to information security is still lacking (Doyle et al., 2025).

In countries with high-intensity digital communication use and complex political dynamics, these processes are particularly important. The information environment is becoming more sensitive to manipulative narratives, emotionally charged content, and coordinated communication campaigns aimed at influencing public sentiment. In this regard, the issue of information security goes beyond the purely technical protection of information systems and is increasingly linked to the resilience of communication processes and the ability of society to critically perceive information flows.

Despite a significant number of studies devoted to digital media and the transformation of communication practices, most consider only certain aspects of the problem—technological, sociopsychological, or political. Moreover, a systematic approach to the comprehensive identification of information security risks in the modern media space remains underdeveloped. In this context, the aim of the study is to analyze the peculiarities of public communication in the digital media environment, systematize key threats to information security, and justify methodological approaches to the analytical assessment of modern information flows.

2. Materials and Methods

2.1. Research strategy and conceptual framework

The methodology of this study is structured as a systematic analytical reconstruction of the processes that shape information security risks in the public media communication environment. We deliberately rejected a narrowly technical approach. The focus is on the interaction between digital platforms, algorithmic mechanisms, and social responses from the audience. It is this triad that defines the current configuration of threats. The study design is combined in nature. It combines a systematic search for scientific sources, an analysis of open statistical data, a content analysis of analytical publications, and the construction of a risk classification model.

This multilevel structure moves from describing individual incidents to identifying patterns. In short, we are not investigating events but rather structure (Figure 1).

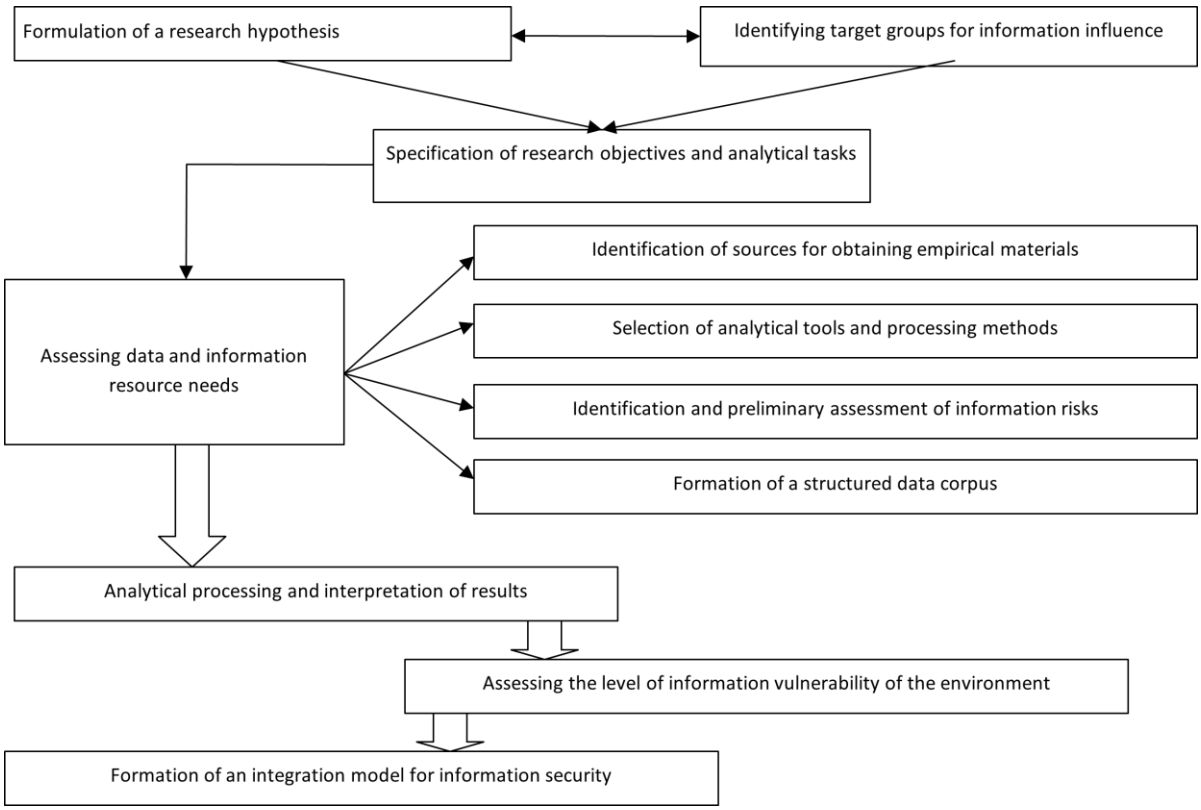

Figure 1 Logical-procedural diagram of the formation and implementation of the methodological research model.

2.2. Formation of the corpus of sources and data

The search for scientific materials was conducted in the international databases Scopus, Web of Science, and Google Scholar for the period from 2015–2025. The choice of period was determined by the active platformization of the communication space and the growth of algorithmic influence on information flows. The search formulas included combinations of the descriptors "information security," "public media communication," "hybrid threats," "disinformation," and "algorithmic amplification." The logical operators AND and OR were used. The analysis was conducted on the basis of titles, abstracts, and keywords. In addition to academic sources, the analysis included open statistical reports from international research centers on the structure of news consumption, trust in the media, and the share of social networks in the dissemination of information.

2.3. Selection procedure and analytical logic

The materials were selected in three consecutive phases: identification, screening, and full-text assessment. The principle of double-checking was applied at each stage. Two researchers conducted an independent assessment of relevance. Disagreements were resolved through reanalysis of the arguments. The inclusion criteria were as follows:

1. The presence of an analysis of threats to information security.
2. A link to public media communication.
3. An empirical or statistical basis.
4. A clearly described methodology.

Declarative materials without analytical tools were excluded (Table 1).

Table 1 Stages and tools of the methodological procedure.

Stage	Object of analysis	Method	Evaluation criteria	Result
Identification	Publications 2015–2025	Bibliographic search	Thematic relevance	Primary array
Elimination of repetitions	Bibliographic records	Technical inspection	Duplication	Optimized database
Screening	Abstracts	Thematic analysis	The presence of a security dimension	Abbreviated sample
Full-text evaluation	Full texts	Critical expertise	Methodological clarity	Final casing
Content analysis	Analytical fragments	Categorization	Repetition of threats	Risk typology
Statistical interpretation	Report data	Comparative analysis	Share of news consumption	Dynamics of change
Modeling	Summary results	Analytical reconstruction	Consistency of levels	Conceptual diagram

2.4. Methods of threat classification

Content analysis was employed to identify recurring risk categories, including algorithmic amplification of manipulative content, disinformation campaigns, information and psychological operations, cyber incidents, and institutional vulnerability. The unit of analysis was defined as an analytical fragment (paragraph-level argument) extracted from the selected corpus. In total, coded fragments were analyzed. The frequency of each category was calculated as the percentage of its occurrence within the total number of coded units.

The coding procedure consisted of two stages: open coding to identify primary categories and axial coding to group them into higher-order structures. To ensure reliability, a subset of the material (20%) was independently coded, with intercoder agreement reaching Cohen's κ = [0.7–0.85], indicating acceptable consistency. Classification was carried out according to a hierarchical principle. At the first level, technological factors were identified. The second level included socio-psychological consequences, such as polarization and declining trust in media. The third level captured political and international dimensions. This multi-level structure enabled the identification of cause–effect relationships between technological drivers and societal outcomes.

Bibliometric analysis supplemented the classification by identifying the most frequently studied threat categories, thereby revealing the concentration of academic attention and existing research gaps.

2.5. Integrative risk modeling

The final stage involved the construction of an integrated analytical model designed to capture the systemic nature of information security risks. The model is structured around three interconnected analytical levels. The technological level includes algorithmic mechanisms acting as structural regulators of information flows. These are operationalized through

engagement-based indicators, such as content reach and interaction intensity, which serve as proxies for algorithmic amplification. The communicative level reflects the dynamics of information dissemination and is assessed through the frequency and distribution of manipulative content identified in the coded corpus. This level captures the intensity and typology of information flows. The socio-psychological level represents audience responses, including polarization and declining trust in media, approximated through indicators derived from analytical reports and recurring thematic patterns in the dataset. The integration of these levels enables a semi-quantitative assessment of risk interactions. Changes in one dimension (e.g., increased algorithmic amplification) are modeled as producing cascade effects across communicative and social levels, thereby shaping the overall risk profile. To ensure internal consistency, the model was validated through reanalysis of key categories and comparison with international statistical reports, confirming the alignment of identified patterns with empirical trends.

3. Results and Discussion

The analysis of the coded corpus shows that the current media environment is characterized by multiple communication pathways that significantly accelerate information dissemination, while digital platforms now act as dominant intermediaries that structure the way in which government institutions interact with media outlets and their public audience. Social media have emerged as the primary environment for public engagement and opinion formation, enabling users both to consume information and to construct alternative narratives that may challenge official positions (Ng et al., 2025).

Our results indicate that the process of developing communication strategies now depends increasingly on digital indicators and analytical tools, which enable real-time monitoring of audience sentiment and adaptive content adjustment (Subaveerapandiyan et al., 2025). At the same time, algorithm-driven platforms demonstrate a dual effect: they enhance information accessibility while simultaneously generating systemic risks, including the formation of algorithmically reinforced information bubbles and the amplification of manipulative or distorted content (Hulland, 2024).

At the communicative level, the analysis reveals a clear shift toward the dominance of visual and multimedia formats. Compared with traditional text-based communication, video content, infographics, and interactive visualizations exhibit higher emotional impact and engagement intensity, thereby increasing their influence on mass perception (Mardiani et al., 2024).

The evolving communication environment requires the development of advanced media literacy and critical thinking skills as adaptive societal responses. The results further demonstrate the hybridization of information influence, where authentic communication practices are combined with deceptive tactics, creating complex and difficult-to-distinguish information environments. The spread of false information, propaganda content, and automated social media accounts serves as a key mechanism of such hybrid influence (Terchila, 2025; Torres-Salinas, 2024).

Overall, the findings indicate that the modern media environment functions as an integrated system shaped by digital technology, personalized information flows, and the growing dominance of visual and emotional content. While these trends expand opportunities for information democratization, they also increase vulnerability to manipulative influence and reduce the predictability of public opinion formation. In this context, the analysis highlights the need for specialized risk assessment approaches capable of capturing both the structural dynamics of information flows and their socio-psychological effects. The distribution of identified threats, derived from frequency analysis of coded categories, is presented in Table 2.

Analysis of digital media and social networks reveals that the main threats to information security are related to the manipulative nature of information flows, algorithmic limitations, and hybridization of information influences. They can not only create a distorted information environment but also pose long-term risks to social stability and democratic processes.

Manipulative technologies in modern media communications are becoming systemic and are used to achieve political, economic and social goals. They are manifested through various channels—from traditional media to social networks and digital platforms. For a comprehensive analysis, generalized mechanisms of manipulation are presented in Table 3.

Mechanisms of manipulative technologies in the media space demonstrate high flexibility and the ability to adapt to new communication conditions. Their actions are aimed at forming controlled interpretations of reality, which leads to increased polarization of society, undermining trust in democratic institutions, and increasing information threats. This influence complicates the formation of an objective information environment, increasing risks to information security at the global level (Makedon et al., 2025a).

Recent studies confirm that social media is becoming a leading channel for receiving news in different countries. Moreover, the scale and intensity of platform use vary considerably from region to region. The study summarized international statistics and created a graph showing the level of news consumption through social media (see Figure 2). The data for the figure were obtained from open international statistical sources specializing in media consumption research (Pew Research Center, Reuters Institute, DataReportal, etc.). The methodology included a comparative analysis of different countries and regions based on key indicators. Three main variables, namely, social media news consumption rates among the population and platform-specific usage patterns and worldwide news consumption patterns, are examined. The research revealed common patterns that existed together with unique elements that distinguished each nation.

Table 2 Key risks and threats to information security in the modern media space.

Risk category	Nature of the threat	Example of manifestation
Disinformation and fakes	Mass dissemination of false messages that distort reality	Use of botnets to manipulate public opinion (Ng et al., 2025)
Algorithmic manipulations	Formation of «information bubbles» through recommendation algorithms	Increased radicalization and polarization (Hulland, 2024)
Cyber threats	Use of social media as a tool for infrastructure attacks	Phishing, data leaks, cyberattacks on public services (Subaveerapandiyan et al., 2025)
Manipulative content	Use of emotionally charged materials to influence the audience	Propaganda videos, memes, visual campaigns (Mardiani et al., 2024)
Hybrid information attacks	Combining legitimate and illegitimate information practices	Coordination of disinformation campaigns (Torres-Salinas, 2024)
Undermining trust in the media	Systematic reduction of the legitimacy of official sources of information	Campaigns against independent media (Zhang, 2024)

Table 3 Main mechanisms of manipulative technologies in the media space and their impact on the information environment.

Mechanism of manipulation	The essence of the technology	Impact on the information environment
Fake news	Creation and dissemination of fictitious facts	Formation of a distorted reality, loss of trust in official sources (Ng et al., 2025)
Clickbait	Using sensationalized headlines to attract attention	Increasing emotionality and reducing analytical perception (Hulland, 2024)
Emotional visualization	Emphasis on images that evoke strong emotions	Manipulation of moods and collective behavior (Mardiani et al., 2024)
Bots and trolls	Use of automated accounts to scale messages	Artificially creating social consensus or division (Torres-Salinas, 2024)
Algorithmic prompts	Use of algorithms to create individualized news feeds	Creating information bubbles and polarizing society (Lim & Kumar, 2024)
Information attacks	Coordination of disinformation campaigns in hybrid wars	Undermining national security and international stability (Zhang, 2024)

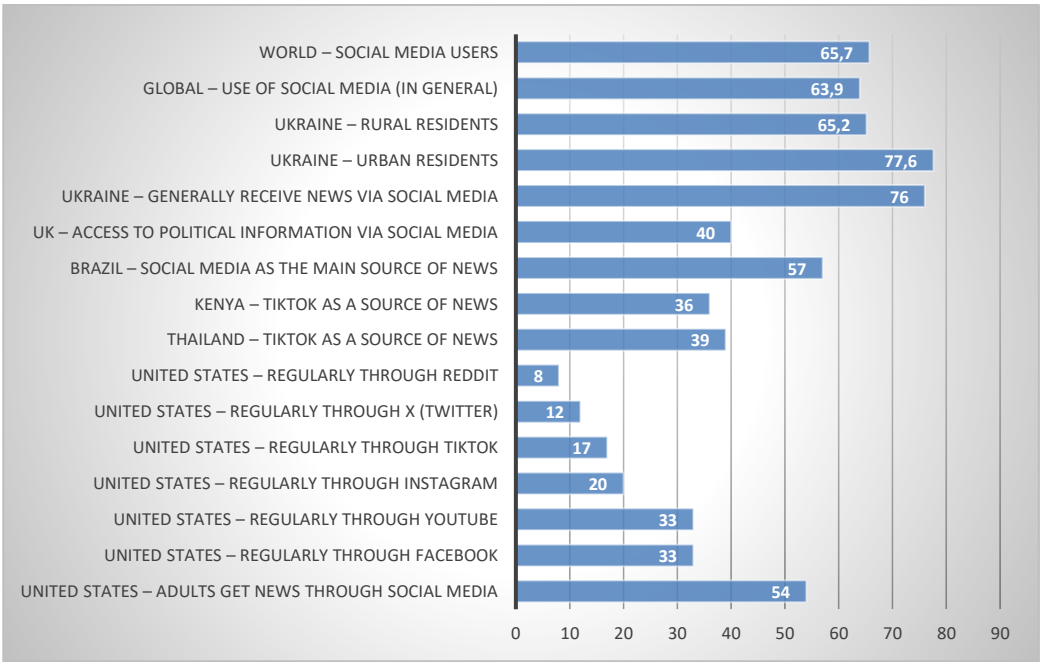

Figure 2 Use of social media as a source of news in different countries and around the world, %.
Source: created by the author based on Hulland, 2024; Lim & Kumar, 2024; Mardiani et al., 2024; Ng et al., 2025; Torres-Salinas, 2024; Zhang, 2024.

The research data show that social media operates as a news platform with distinct characteristics across different countries worldwide. The survey revealed that Ukraine had the highest percentage of people who used the internet, with the

percentage of urban residents reaching 77.6% and the entire adult population reaching 76%. The percentage of social media users who access Facebook exceeds both the worldwide average of 63.9% and the total number of social media users across the globe, which stands at 65.7%. This means that compared with the average global user, the Ukrainian audience is more actively integrating social media into their news consumption.

Moreover, in rural areas of Ukraine, the figure is lower (65.2%), almost 12.4 percentage points less than that in urban areas. The Brazilian population receives their news primarily through social media platforms at a rate of 57%, which is 19 percentage points lower than that of the Ukrainian population. The United States accounts for 54% of adult news consumption through social media, but this figure is 22.6 points lower than that of Ukraine, while social media platforms continue to dominate how people obtain their news. Disaggregation by platform shows that Facebook and YouTube have the same share (33%), while Instagram and TikTok are inferior, with 20% and 17%, respectively.

Moreover, X (Twitter) is used by only 12% of the population, and Reddit is even less popular at 8%. These findings indicate that news consumption in the U.S. is spread across several platforms, whereas in Ukraine, the general level of social media use does not significantly differ. Interesting trends are observed in the countries of the Global South. In Thailand, 39%, and in Kenya, 36% of the population uses TikTok as a source of news. These figures are twice as high as those in the United States (17%), which demonstrates the rapid growth of the role of new platforms among young people in Asia and Africa. In the UK, 40 percent of respondents indicated social media as a source of political information, which confirms its importance in shaping public opinion during elections, but this figure is still lower than the Ukrainian level of news consumption through social media.

In general, in countries with a high level of political turbulence and active digital communities (e.g., Ukraine), social media is a more important source of news than it is in countries with established media systems (the United States and the United Kingdom). The increase between the leading and lagging countries is more than 20 percentage points, which indicates that societies are differently dependent on digital platforms as the main channel of information (Siuta et al., 2021).

The growth of hybrid threats and the active spread of disinformation campaigns require a clear classification of the challenges faced by the modern information security system. These challenges cover both technological and social aspects, which creates a complex multilevel risk environment. To systematize such problems, Table 4 presents the main groups of challenges.

Table 4 Classification of the main challenges for the information security system in modern media space

Category of challenge	Content and examples of manifestations	Potential consequences
Technological	Use of artificial intelligence to create deepfakes, automated bot farms	Massive spread of fake news, undermining trust in authentic sources (Xu et al., 2024)
Information and communication	Manipulation of recommendation algorithms, creation of information bubbles	Polarization of society, reduction of critical thinking (Lim & Kumar, 2024)
Social and psychological	Use of emotionally charged content, propaganda campaigns	Formation of distorted public opinion, radicalization of certain groups (Mardiani et al., 2024)
Political	Coordinated disinformation campaigns during election periods or crises	Undermining the legitimacy of institutions, destabilizing public administration (Ng et al., 2025)
Cybersecurity	Cyberattacks through social platforms, hacking of accounts and infrastructure	Theft of personal data, paralysis of digital services (Subaveerapandiyan et al., 2025)
International	Use of transnational information campaigns in hybrid wars	Impact on global security, spreading distrust of international partners (Torres-Salinas, 2024)

Source: created by the author based on Subaveerapandiyan et al., 2025; Lim & Kumar, 2024; Mardiani et al., 2024; Ng et al., 2025; Torres-Salinas, 2024; Xu et al., 2024.

The classification of challenges reveals that the information security system is under multidirectional pressure—from technological innovations to international disinformation campaigns. Technological and communication factors form the basis for new threats, while sociopsychological and political aspects increase their impact on public consciousness. Combined with cyber threats and the international dimension, this creates an environment of increased vulnerability that requires a systemic response at the national and global levels (Makedon et al., 2025b).

An analytical assessment of information flows in the modern media space requires the integration of digital indicators and statistical methods to obtain an objective picture of the impact of communications. It is based on a combination of quantitative and qualitative indicators, which allows us to study not only the amount of information but also the nature of its distribution and social and psychological effects. The methodological approaches are summarized in Table 5.

Table 5 Methodological approaches to the analytical assessment of information flows in the media space.

Methodological approach	Tools and digital indicators	Examples of use and value
Bibliometric analysis	DOI, citation indices, scientometric databases	Identification of trends in scientific communications and information networks (Donthu, 2021)
Content analysis	Automated text processing systems, keyword and tone analysis	Research on manipulative strategies in social media (Zhang, 2024)
Social network analysis	Graph models, indicators of centrality, density, modularity	Identification of opinion leaders, detection of botnet coordination (Ng et al., 2025)
Statistical modeling	Correlation and regression analysis, ANOVA, time series	Assessing the impact of information flows on public opinion (Hulland, 2024)
Machine learning	NLP models, classification, clustering, transformers	Automated analysis of large data sets to detect disinformation (Xu et al., 2024)
Integrated approaches	Combination of quantitative and qualitative methods, data visualization	Formation of a multidimensional analytical picture of information flows (Marzi et al., 2025)

The proposed methodological approaches reflect the trend toward interdisciplinarity in information flow research. The use of bibliometrics and content analysis helps to identify patterns in the content of messages. Moreover, social network analyses allow us to trace the structure of communication networks, and statistical modeling and machine learning provide in-depth quantitative assessment. Integrated approaches open up opportunities to create a comprehensive picture of the information environment, which is critical in countering disinformation and ensuring information security.

The public communication of authorities needs to be improved through principles that include transparency and evidence-based approaches and efficient delivery. The government needs to maintain continuous citizen updates through official communication channels, which should incorporate digital platforms that present information through text and images and interactive elements. The method will establish public trust in official institutions while minimizing the effects of false information that alternative platforms disseminate. The implementation of information flow monitoring systems represents an effective solution that enables organizations to detect manipulative messages and fakes in real time. Authorities need to create alliances with independent fact-checking organizations that protect the information environment at different levels from propaganda attacks and information distortions (Mialkovska et al., 2022, 2023).

The media and civil society play equally important roles in shaping a threat-resistant information space. The media needs to follow journalistic ethics standards while performing fact-checking operations and remaining away from sensational reporting that enables manipulation. Media literacy education needs improvement from civil society organizations and educational institutions because they should teach students to assess information sources critically since digital content consumption leads young people to become the main audience. The government needs to work with media organizations and civil society groups to develop multiple protective systems that decrease information security threats while building public trust and defending the country against hybrid information-based attacks.

Modern scientific research is actively focusing on the development of bibliometric research methodology, which emphasizes the importance of the DOI as a tool for improving the reliability of scientific works (Alaiaq, 2025; Turki et al., 2023). Some authors propose approaches to minimize citation errors and formulate practical recommendations for researchers (Cioffi et al., 2022; Carrera-Rivera et al., 2022). Research studies have detected patterns in which authors use bibliometric methods for studying knowledge across medical sciences, digital technology and humanistic fields (Ganti et al., 2025; Mardiani et al., 2024; Mirzapour & Sheikhshoaei, 2024; Zhou & Ma, 2025). Such research also focuses on multiple specific areas, including publication ethics analysis (Zhang, 2024) and educational informatics development (Wei et al., 2025).

The literature contains multiple studies that focus on establishing common standards and essential criteria for performing bibliometric reviews (Montazeri et al., 2023; Ng et al., 2025). This research requires both critical result evaluation and interdisciplinary methods according to Lim & Kumar (2024), Öztürk et al. (2024), and Passas (2024). The current literature presents methods that enable researchers to perform systematic bibliometric reviews through step-by-step procedures that unite analysis with synthesis and theory development (Marzi et al., 2025; Donthu, 2021; Hoang, 2025; Kumar, 2025). Several studies have focused on developing new digital methods that use artificial intelligence models to perform automated bibliometric analysis (Xu et al., 2024; Subaveerapandiyan et al., 2025; Blaschke, 2024; Antunes & Veríssimo, 2024).

The current scientific research field dedicates its efforts to bibliometric research methodology development because DOI serves as a vital instrument that guarantees scientific publication reliability and worldwide accessibility (Alaiaq, 2025; Turki et al., 2023). This process requires scientists to identify and fix technical problems that affect scientometric assessment results (Cioffi et al., 2022; Carrera-Rivera et al., 2022). The development of bibliometrics in different fields becomes evident through examples that show how these methods are used in medical research and artistic studies and in cultural analysis and digital technology assessment and educational research (Ganti et al., 2025; Mardiani et al., 2024; Mirzapour & Sheikhshoaei, 2024;

Zhou & Ma, 2025). Particular attention is given to the ethics of publications (Zhang, 2024), as well as the historical development of informatics in the focus of leading international publications (Wei et al., 2025). In this context, domestic researchers also emphasize the integration of digital media into the process of forming competencies in higher education (Batsurovska et al., 2021).

An important area is the development of standards and guidelines for conducting bibliometric reviews, among which international initiatives to create minimum requirements and agreed reporting rules stand out (Montazeri et al., 2023; Ng et al., 2025). Researchers emphasize the need to critically reflect on the results and avoid a simplistic approach to data interpretation (Lim & Kumar, 2024; Öztürk et al., 2024; Passas, 2024). The research by Öztürk et al. (2024) proposed a conceptual framework for designing bibliometric studies that systematizes the stages of planning, selection of sources and methods. We can argue that such an approach increases the reproducibility of the results. Research conducted by Antunes and Veríssimo (2024) shows that bibliometrics serve as an operational system that identifies sensory marketing patterns. Blaschke (2024) developed an authorship analysis method for scientific papers, which led researchers to stop using their previous citation-based evaluation approach. The Ukrainian context is presented by Batsurovska et al. (2021), who investigate the formation of competencies in the digital educational environment. Their work is an accurate example of the integration of bibliometric and communication approaches in the training of future professionals.

Recent works have formulated step-by-step algorithms for bibliometric systematic reviews and comprehensive methodological strategies that integrate analysis, synthesis, and theory development (Marzi et al., 2025; Donthu, 2021; Hoang, 2025; Kumar, 2025). Digital solutions, including automated analysis systems, artificial intelligence, and transformative models that allow the processing of large datasets, are becoming increasingly important (Xu et al., 2024; Subaveerapandiyan et al., 2025; Blaschke, 2024; Antunes & Veríssimo, 2024). Moreover, new directions are emerging, such as narrative bibliometrics, which offer qualitative approaches to reflecting the dynamics of scientific communications (Torres-Salinas, 2024).

The results of the study confirmed the hypothesis that the modern media space is both a source of new opportunities for the democratization of communication and a risk factor for information security. The data analysis revealed the dominant role of social media in shaping public opinion, which is consistent with the findings of Ng et al. (2025) and the Pew Research Center. Moreover, Hulland (2024) emphasizes the danger of algorithmic “information bubbles”, but our results show that in Ukraine, social media is used as the main source of news much more intensively than it is in the United States or the United Kingdom, making the audience even more vulnerable to such effects.

Some authors emphasize the positive potential of digital technologies in ensuring the openness and accessibility of data (Subaveerapandiyan et al., 2025; Marzi et al., 2025), whereas others emphasize hybrid threats and manipulations that increase with the development of such technologies (Torres-Salinas, 2024; Zhang, 2024). The research data show that digital platforms serve as two vital communication systems that enhance public participation, yet they act as botnet-controlled platforms to spread fake news and emotional content.

The research method of Lim and Kumar (2024) uses bibliometric analysis to study information distribution, but our study demonstrates that media space evaluation requires both quantitative and qualitative assessment approaches. However, it is worth noting that the interpretation of the data has limitations related to uneven access to statistical sources and differences in the methodology of international studies.

The results show that modern information systems function as complex networks that enable data transmission between various system components. The research findings match those of worldwide studies, but Ukrainian society shows extreme social media usage, which makes information security more vulnerable. Research needs to continue to create complete models that protect against hybrid threats while making media literacy part of educational and communication system infrastructure.

4. Final Considerations

Our research revealed how modern public communication operates through multiple channels that simultaneously enhance democratic processes and generate systemic security risks, enabling democratic processes while also creating structural vulnerabilities shaped by the interaction of technological, communicative, and social factors. The results indicate that algorithmic amplification and disinformation represent the most structurally significant threats, particularly in environments characterized by high levels of social media engagement, such as Ukraine. The study demonstrates that Ukrainian users actively engage with social media as a primary source of news, which increases exposure to algorithmically amplified manipulative content.

Our research achieves its originality by integrating quantitative analysis of international statistical data with qualitative risk classification, thereby enabling the development of a comprehensive analytical framework for assessing media space dynamics. Our findings have practical value as they support the development of state information security strategies, media literacy programs, and systems for monitoring manipulative content.

The results obtained suggest the need to reconsider the architecture of information security management. Rather than focusing solely on reactive responses, it is necessary to redefine the principles of regulating the digital communication environment. Public media communication increasingly functions under conditions of algorithmic mediation, which means

that algorithmic governance becomes an integral component of security policy. The implications are multilayered. At the institutional level, there is a need to create mechanisms for independent algorithmic auditing. At the level of media organizations, there is a need to develop internal protocols for verifying sources and monitoring information flows. At the societal level, digital literacy is becoming increasingly important. Without it, no regulatory measures will have a lasting effect.

The prognostic dimension is also ambivalent. On the one hand, increased automation may increase the scale of manipulative campaigns. On the other hand, the development of artificial intelligence tools provides opportunities for the early detection of information attacks. Thus, the future trajectory of information security systems will depend on the ability to balance technological innovation with the principles of transparency and accountability.

4.1. Limitations

The study is based primarily on secondary data and literature analysis, which limits the empirical depth of the findings. The absence of primary empirical research constrains the robustness and external validity of the conclusions. Future studies incorporating original data collection, such as surveys, experiments, or media content analysis, could strengthen the evidential basis and enhance the overall validity of the results.

5. Declarations

5.1. Ethical considerations

Not applicable.

5.2. Use of artificial intelligence (AI)

The authors declare that no generative artificial intelligence tools were used in the preparation, analysis, or writing of this manuscript.

5.3. Conflict of interest

The authors declare that they have no conflicts of interest.

5.4. Funding

This research did not receive any financial support.

References

Alaiaq, A. S. (2025). The importance of the digital object identifier (DOI) in enhancing the credibility of scientific research: An analytical data study. *arXiv*. https://doi.org/10.48550/arXiv.2508.20118

Antunes, I. F. S., & Veríssimo, J. M. C. (2024). A bibliometric review and content analysis of research trends in sensory marketing. *Cogent Business & Management, 11*(1), 2338879. https://doi.org/10.1080/23311975.2024.2338879

Batsurovska, I., Dotsenko, N., Gorbenko, O., & Kim, N. (2021). The technology of competencies acquisition by bachelors in higher education institutions in the conditions of the digital media communication environment. In *Proceedings of the International Conference on New Trends in Languages, Literature and Social Communications (ICNTLLSC 2021)* (pp. 206–213). Atlantis Press. https://doi.org/10.2991/assehr.k.210525.025

Blaschke, S. (2024). Publication authorship: A new approach to the bibliometric study of scientific work and beyond. *PLOS ONE, 19*(4), Article e0297005. https://doi.org/10.1371/journal.pone.0297005

Carrera-Rivera, A., Ochoa, W., Larrinaga, F., & Lasa, G. (2022). How-to conduct a systematic literature review: A quick guide for computer science research. *MethodsX, 9*, 101895. https://doi.org/10.1016/j.mex.2022.101895

Cioffi, A., Coppini, S., Massari, A., Moretti, A., Peroni, S., Santini, C., & Shahidzadeh Asadi, N. (2022). Identifying and correcting invalid citations due to DOI errors in Crossref data. *Scientometrics, 127*, 3593–3612. https://doi.org/10.1007/s11192-022-04367-w

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research, 133*, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Doyle, G., Barr, K., & Boyle, R. (2025). Public service media as critical media infrastructure for the digital era. *Media, Culture & Society, 47*(6), 1132–1149. https://doi.org/10.1177/01634437251330119

Ganti, L., Persaud, N. A., & Stead, T. S. (2025). Bibliometric analysis methods for the medical literature. *Academic Medicine & Surgery*. https://doi.org/10.62186/001c.129134

Goncharuk-Cholach, T., Rudakevych, O., Lazarovych, M., Huryk, M., & Chyhur, R. (2025). Digital resistance in authoritarian realities and technologies of political changes. *Evropský politický a právní diskurz, 12*(4), 20–31. https://doi.org/10.46340/eppd.2025.12.4.3

Hoang, A.-D. (2025). Evaluating bibliometric reviews: A practical guide for peer review and critical reading. *Evaluation Review, 49*(6), 1074–1102. https://doi.org/10.1177/0193841X251336839

Hulland, J. (2024). Bibliometric reviews—Some guidelines. *Journal of the Academy of Marketing Science, 52*, 935–938. https://doi.org/10.1007/s11747-024-01016-x

Kumar, R. (2025). Bibliometric analysis: Comprehensive insights into tools, techniques, applications, and solutions for research excellence. *Spectrum of Engineering and Management Sciences, 3*(1), 45–62. https://doi.org/10.31181/sems31202535k

Lim, W. M., & Kumar, S. (2024). Guidelines for interpreting the results of bibliometric analysis: A sensemaking approach. *Global Business and Organizational Excellence, 43*(3), 17–26. https://doi.org/10.1002/joe.22229

Makedon, V., Myachin, V., Aloshyna, T., Cherniavska, I., & Karavan, N. (2025a). Improving the readiness of enterprises to develop sustainable innovation strategies through fuzzy logic models. *Economic Studies (Ikonomicheski Izsledvania), 34*(5), 165–179.

Makedon, V., Myachin, V., Kuriacha, N., Chaika, Yu., & Koptilyi, D. (2025b). Development of strategic management of a corporation through the implementation of scenario analysis. *Scientific Bulletin of Mukachevo State University. Series "Economics", 12*(2), 135–146. https://doi.org/10.52566/msu-econ2.2025.135

Makedon, V., Zaikina, H., Slusareva, L., Shumkova, O., & Zhmaylova, O. (2020). Use of rebranding in marketing sphere of international entrepreneurship. *International Journal of Entrepreneurship, 24*(1S). https://www.abacademies.org/articles/use-of-rebranding-in-marketing-sphere-of-international-entrepreneurship-9325.html

Mardiani, E., Rukmana, A. Y., Maqfirah, P. A. V., Nuswantoro, P., & Uhai, S. (2024). Bibliometric study on the influence of digital technology in the field of arts and culture. *The Eastasouth Journal of Social Science and Humanities, 1*(2), 58. https://doi.org/10.58812/esssh.v1i02.212

Marzi, G., Balzano, M., Caputo, A., & Pellegrini, M. M. (2025). Guidelines for bibliometric-systematic literature reviews: 10 steps to combine analysis, synthesis and theory development. *International Journal of Management Reviews, 27*(1), 81–103. https://doi.org/10.1111/ijmr.12381

Mialkovska, L., Yanovets, A., Solohub, L., Pochapska, O., & Reshetnik, H. (2022). Cognitive and pragmatic aspects of media text in the digital context. *IJCSNS International Journal of Computer Science and Network Security, 22*(1), 485–490. https://doi.org/10.22937/IJCSNS.2022.22.1.63

Mialkovska, L., Yanovets, A., Sternichuk, V., Nykoliuk, T., Honchar, K., & Khnykina, O. (2023). Manipulative tactics in modern English-language media discourse. *Conhecimento & Diversidade, 15*(38), 345–362.

Mirzapour, L., & Sheikhshoaei, F. (2024). Bibliometric study of *BioImpacts* using a technological impact approach. *BioImpacts, 15*, 30401. https://doi.org/10.34172/bi.30401

Montazeri, A., Mohammadi, S., Hesari, P. M., Ghaemi, M., Riazi, H., & Sheikhi-Mobarakeh, Z. (2023). Preliminary guideline for reporting bibliometric reviews of the biomedical literature (BIBLIO): A minimum requirements. *Systematic Reviews, 12*(1), 239. https://doi.org/10.1186/s13643-023-02410-2

Ng, J. Y., Liu, H., Masood, M., Syed, N., Stephen, D., Ayala, A. P., Sabé, M., Solmi, M., Waltman, L., Haustein, S., & Moher, D. (2025). Guidance for the reporting of bibliometric analyses: A scoping review. *Quantitative Science Studies, 6*, 988–1001. https://doi.org/10.1162/qss.a.12

Öztürk, O., Kocaman, R., & Kanbach, D. K. (2024). How to design bibliometric research: An overview and a framework proposal. *Review of Managerial Science, 18*(11), 3333–3361. https://doi.org/10.1007/s11846-024-00738-0

Passas, I. (2024). Bibliometric analysis: The main steps. *Encyclopedia, 4*(2), 1014–1025. https://doi.org/10.3390/encyclopedia4020065

Siuta, H., Mialkovska, L., Ivanenko, I., Syrko, I., Senkovych, O., & Sobol, L. (2021). Precedent names in the language of modern Ukrainian journalism. *Ad Alta: Journal of Interdisciplinary Research, 11*(2), 91–95.

Subaveerapandiyan, A., Taj, A., & Nair, A. R. (2025). Advancing open science: A bibliometric study of scholarly metadata research (1995–2024). *Science & Technology Libraries, 45*(1), 100–129. https://doi.org/10.1080/0194262X.2025.2517089

Terchila, S. (2025). External communication in the public and private sectors of the European Union: Impact on business owners, clients, and communities. *Proceedings of the International Conference on Business Excellence, 19*(1), 4429–4442. https://doi.org/10.2478/picbe-2025-0339

Torres-Salinas, D., Orduña-Malea, E., Delgado-Vázquez, Á., Gorraiz, J., & Arroyo-Machado, W. (2024). Foundations of narrative bibliometrics. *Journal of Informetrics, 18*(3), 101546. https://doi.org/10.1016/j.joi.2024.101546

Turki, H., Fraumann, G., Hadj Taieb, M. A., & Ben Aouicha, M. (2023). Global visibility of publications through digital object identifiers. *Frontiers in Research Metrics and Analytics, 8*, 1207980. https://doi.org/10.3389/frma.2023.1207980

Wei, W., Huang, X., Zhang, S., Wang, W., & Liu, M. (2025). *Journal of Informetrics* 2007–2023: A retrospective bibliometric analysis. *SAGE Open, 15*(3). https://doi.org/10.1177/21582440251361875

Xu, H., Li, X., Tupayachi, J., Lian, J., & Omitaomu, F. (2024). Automating bibliometric analysis with sentence transformers and retrieval-augmented generation (RAG): A pilot study in semantic and contextual search for customized literature characterization for high-impact urban research. *arXiv Preprint*, arXiv:2410.09090. https://doi.org/10.48550/arXiv.2410.09090

Zhang, M., Xu, J., Xu, C., Zheng, Q., Liu, M., Zhang, J., Fu, H., Qi, W., Zhang, J., & Tian, J. (2024). Bibliometric review and mapping analysis of publication ethics research. *Ethics & Behavior, 34*(6), 397–409. https://doi.org/10.1080/10508422.2024.2306134

Zhou, C., & Ma, L. (2025). Bibliometric insights into the top 100 most-cited annual studies on digital health in nursing education (2020–2024). *Digital Health, 11*. https://doi.org/10.1177/20552076251342165