



Mapping the intellectual structure of intelligence communication studies in national security contexts: A bibliometric approach

Hasdiyanto Hafied^{*,†}, Andi Alimuddin Unde[†], Syamsuddin Aziz[†], Muhammad Farid[†]

Department Communication Sciences, Hasanuddin University, South Sulawesi 90245, Indonesia

Article Info

Article history:

Received 11 July 2024

Revised 07 December 2024

Accepted 16 December 2024

Available online 18 March 2026

Keywords:

bibliometric,
communication,
intelligence,
national security,
scopus

Abstract

This bibliometric study aims to map the knowledge structure and research trends related to “national security” and “intelligence communications”. Using citation, co-citation, and author collaboration analyses, the study provides insights into the intellectual structure of this important field. The findings reveal key themes and subtopics that are gaining attention, such as the impact of technology on the collection and dissemination of intelligence information, the role of communications in intelligence operations, and ethical and legal considerations related to intelligence communications. In addition, the study identified important patterns in author collaboration, indicating a trend toward cross-disciplinary research and knowledge exchange. The bibliometric analysis also reveals opportunities for further research, such as the role of social media and digital platforms in shaping public perceptions of national security and the impact of artificial intelligence and machine learning on intelligence communications. By mapping the research landscape, this study contributes to a deeper understanding of the concepts, theories, and methodologies that shape intelligence communication in the context of national security while highlighting potential future research directions.

© 2026 Kasetsart University.

Introduction

Mapping the intellectual structure of intelligence communication studies in the context of national security through a bibliometric approach involves using quantitative methods to analyze bibliographic data extracted from research studies to identify publishing patterns and trends in a particular knowledge domain

(Chen et al., 2023). This approach enables the identification of a core of theoretical and empirical research in the field, which sheds light on the intellectual structure of the field under study (Ellili, 2024). Using bibliometric analysis, researchers can gain valuable insights into the research area by using bibliographic information from academic publications provided by bibliographic data providers (Kammerer et al., 2021).

* Corresponding author.

E-mail address: hafiedh22e@student.unhas.ac.id (Hafied, H.).

† Co-first authors.

Intelligence communication is a systematic process of collecting, analyzing, and verifying relevant information in the context of national security, which forms an important basis for developing strategic decisions and implementing actions. It deals not only with the technical aspects of information dissemination, but also with the organizational dynamics of information dissemination among security agencies. In the modern context, communication has shifted from the traditional hierarchical model to complex multidimensional networks, which complicates security issues (Eriksson, 2018).

Mapping the intellectual structure of this research domain is crucial to understanding the complex landscape of intelligence communication and identifying critical areas for further exploration. By mapping the intellectual structure of this research domain, we aim to contribute to a deeper understanding of the key concepts, theories, and methodologies that shape intelligence communication in the context of national security. To achieve a comprehensive knowledge of intelligence communication in national security, it is crucial to investigate the various dimensions of this field. We can gain insight into the evolving dynamics and challenges that shape intelligence communications by analyzing key concepts, theories, and methodologies. Moreover, mapping the intellectual structure of this research domain will provide a roadmap for future research, allowing academics and practitioners to identify gaps in knowledge and areas that need to be further explored.

Despite the growing significance of intelligence communication to national security, there remains a critical gap in our understanding of how the field has evolved intellectually and structurally. While individual studies have examined specific aspects of intelligence communication, there has been limited systematic analysis of:

- (1) the theoretical foundations and scholarly structures of the field,
- (2) the evolution of research topics and methodological approaches,
- (3) patterns of knowledge exchange and scholarly collaboration, and
- (4) emerging research frontiers in the digital age.

This knowledge gap hinders our ability to understand the evolution of the field and to identify promising areas for future research.

This study aims to address these gaps through a comprehensive bibliometric analysis of intelligence communication research in national security contexts. Specifically, this research seeks to map the intellectual structure and evolution of intelligence communication studies while identifying major research clusters and their interconnections within the field. Through detailed

analysis of scholarly works, this study examines patterns of collaboration and knowledge exchange among researchers and institutions. Furthermore, this research aims to highlight emerging research themes and potential future directions, providing a roadmap for future scholarly investigation in this critical domain. By undertaking this comprehensive analysis, we seek to contribute to a deeper understanding of how intelligence communication research has evolved and where it may be headed in the context of national security studies.

Bibliometric analysis reveals critical trends in intelligence communication studies in national security. By examining the frequency of citations, co-citations, and author collaborations, this study provides insights into the intellectual structure of this critical field of research.

Identifying key themes and subtopics in the field provides a valuable roadmap for future research directions. This highlights the need to delve deeper into specific areas such as propaganda and influence campaigns, cybersecurity and information warfare, and the ethical implications of intelligence communications. The findings underscore the dynamic and evolving nature of intelligence communication studies in national security, advocating for continued scholarly exploration and interdisciplinary collaboration in this critical domain.

The significance of this study extends across multiple dimensions of intelligence communication research and practice. By providing a systematic understanding of the field's development, this research offers valuable insights into how intelligence communication has evolved within national security contexts. This comprehensive mapping serves as a guide for future research directions while facilitating more effective collaboration between researchers and practitioners in the field. Moreover, the findings of this study carry important implications for policy development and practical applications in intelligence communication. This thorough analysis of the intellectual landscape contributes not only to theoretical advancement but also to practical applications in the field of intelligence communication within national security contexts, bridging the gap between academic research and real-world implementation of intelligence communication strategies.

Literature Review

Current State of Intelligence Communication Research

Conceptual evolution of intelligence communication

Intelligence communication has evolved significantly from its traditional roots in military and diplomatic

contexts to its current role in comprehensive national security frameworks. Early literature focused primarily on hierarchical information flows and formal communication channels (Best, 2015). However, contemporary research has expanded to encompass digital transformation, cybersecurity considerations, and emerging technological challenges (Degaut, 2016; Lindsay, 2020).

Core themes in intelligence communication research

The literature reveals several dominant themes that have shaped the field. Intelligence communication plays a vital role in enabling different agencies and organizations to collaborate and share critical information to prevent and mitigate security threats. Studies by Broniatowski (2019) emphasize that effective communication within the intelligence community is essential for the timely and accurate dissemination of intelligence, ensuring decision-makers have the necessary information to address potential security risks.

Intelligence communication is vital in national security. It enables different agencies and organizations to collaborate and share critical information to prevent and mitigate security threats. Effective communication within the intelligence community is essential for the timely and accurate dissemination of intelligence, ensuring that decision-makers have the necessary information to address potential security risks (Broniatowski, 2019).

Emerging research directions

Recent technological advances have significantly impacted intelligence communications, increasing the speed and efficiency of information sharing (Degaut, 2016). However, these advances also present new challenges, such as ensuring the security and integrity of sensitive intelligence data. The role of intelligence communications has expanded to include not only traditional military and geopolitical threats but also new issues such as cybersecurity, terrorism, and transnational crime (Bury & Chertoff, 2020; Vogel & Tyler, 2019).

In recent years, technological advances have significantly impacted intelligence communications, increasing the speed and efficiency of information sharing (Degaut, 2016). However, these advances also present new challenges, such as ensuring the security and integrity of sensitive intelligence data. The role of intelligence communications in national security has expanded to include traditional military and geopolitical threats and new issues such as cybersecurity, terrorism, and transnational crime. As a result, the intelligence community must continue to adapt and develop new strategies for communication and collaboration to address

these evolving threats effectively (Bury & Chertoff, 2020; Vogel & Tyler, 2019).

In the future, researchers and practitioners must continue to explore and improve intelligence communication practices, considering the changing nature of security threats and the rapid development of communication technologies. By doing so, the intelligence community can better fulfill its mandate to protect national security in an increasingly complex and interconnected world (Bullock et al., 2018).

Bibliometric Studies in Intelligence and Security Research

While bibliometric approaches have been widely used across various disciplines, their application to intelligence communication studies has been limited. Notable examples from related fields include studies by Anwar et al. (2018) on national security research trends and Kammerer et al. (2021) on intelligence research networks.

In addition to technological advances, the importance of human intelligence and the role of analysts in interpreting and contextualizing information must be considered. As technology evolves, it is imperative to balance the use of automated tools for data analysis and the expertise of human intelligence professionals who can provide critical insight and understanding (Regens, 2019).

Effective interagency collaboration and information sharing remain top priorities. Developing standard protocols and platforms for secure communication and data exchange between different intelligence agencies and national security organizations is essential. This ensures a cohesive and coordinated approach to addressing security threats.

Research Gaps Identified in Literature

The comprehensive review of existing literature reveals several significant gaps in current research that need to be addressed. First, there is a limited systematic analysis of the field's intellectual structure. While individual studies have examined specific aspects of intelligence communication, there has been no comprehensive attempt to map the overall intellectual architecture of the field. As noted by Eriksson (2018), this lack of systematic understanding hampers our ability to identify key theoretical foundations and trace the evolution of critical concepts in intelligence communication studies.

Second, the integration of human intelligence capabilities with technological tools remains insufficiently understood. Despite technological advances highlighted by Degaut (2016) and Regens (2019), there is limited research on how to effectively balance human expertise with automated systems in intelligence communication. This gap is particularly significant as intelligence agencies increasingly rely on both human analysts and artificial intelligence tools for data processing and analysis.

Third, there is a pressing need for better frameworks governing interagency collaboration and information sharing. Current literature, including studies by Bury & Chertoff (2020) and Vogel & Tyler (2019), identifies significant challenges in coordinating intelligence communication across different agencies and organizations. However, research has yet to provide comprehensive frameworks for addressing these challenges, particularly in the context of evolving security threats and technological capabilities.

Fourth, ethical considerations in modern intelligence communication have received limited scholarly attention. While studies by Parsons (2015) and Watt (2017) touch on privacy concerns, there remains a significant gap in research addressing broader ethical implications of modern intelligence communication practices, especially regarding surveillance, data protection, and civil liberties in the digital age.

These identified gaps highlight the necessity for a comprehensive bibliometric analysis that can systematically map the evolving landscape of intelligence communication studies in national security contexts. Such analysis would not only provide a clearer understanding of the field's current state but also identify promising directions for future research. As Cobley & Schulz (2013) suggest, understanding these gaps is crucial for developing more effective and ethically sound approaches to intelligence communication in contemporary security environments.

Additionally, the ethical considerations surrounding intelligence communications in the digital age present an exciting area for future research. As technological advances continue to outpace regulatory frameworks, there is an urgent need to address privacy, surveillance, and the responsible use of communication tactics in intelligence operations (Tosun, 2018).

In addition to these emerging research directions, this analysis emphasizes the importance of interdisciplinary collaboration to address the complex challenges in intelligence communications studies. Combining expertise from fields such as communications, cybersecurity, psychology, and political science can

provide holistic insights and solutions to real-world problems in the field of national security and intelligence operations (Wai, 2020; Willmetts, 2019).

By identifying these potential research directions, bibliometric analyses contribute to the current understanding of intelligence communication in national security and pave the way for continued scholarly exploration and innovative interdisciplinary collaborations. The analyses presented have highlighted the importance of intelligence communication studies in national security. Nevertheless, it is essential to consider the potential drawbacks and ethical issues associated with the intersection of intelligence, communications, and technology.

As the security threat landscape continues to evolve, intelligence communication strategies must not only focus on current threats but also anticipate and prepare for emerging risks. This requires an agile and adaptable communications framework that can pivot to address new challenges as they arise (Bury & Chertoff, 2020).

Continuously evaluating and refining intelligence communication practices allows the intelligence community to proactively stay ahead of security threats and contribute to safeguarding national and global security interests.

Methodology

This research is a bibliometric study that aims to map the knowledge structure and research trends related to “national security” and “intelligence communication.” To achieve this goal, a series of systematic steps have been taken in data collection and analysis.

Firstly, a data search was conducted using the Scopus database, which is one of the largest and most comprehensive bibliographic data sources in the world. Scopus was selected as the primary database for this study due to its comprehensive coverage of social science literature and reliable bibliometric data quality. While specialized security databases exist, Scopus offers broader interdisciplinary coverage essential for understanding intelligence communication research. Additionally, Scopus provides consistent historical coverage spanning our target period (1987-2024) and ensures all indexed journals undergo rigorous peer review processes, enhancing the reliability of our dataset.

The selection period of 1987-2024 was chosen based on several critical considerations. First, 1987 marks a significant turning point with the introduction of major computerization initiatives in intelligence operations. Second, this period captures crucial transformations in

intelligence communication methods, including the post-9/11 security paradigm shift and recent technological innovations. Additionally, this study utilized Scopus Database for statistical analysis, VOSviewer (version 1.6.18) for network visualization and data cleaning processes.

The search query used was (TITLE-ABS-KEY (“national security”) and TITLE-ABS-KEY (intelligence and communication)) and (LIMIT-TO (SUBJAREA, “SOCT”) and (LIMIT-TO (DOCTYPE, “ar”))). This query is designed to identify documents that have the keywords “National security”, “intelligence” and “communication” in the title, abstract, or keywords. This search is limited to journal articles and conference proceedings to ensure the quality and relevance of the documents obtained.

From the search results, 68 documents covering the publication period from 1987 to 2024 were obtained. These documents were then downloaded and processed for bibliometric analysis. The processing of these 68 articles involved several systematic steps. First, bibliographic information including author details, citations, abstracts, and keywords was extracted and standardized. Author names and institutional affiliations were verified and harmonized to ensure consistency. For co-authored articles, special attention was given to recording multiple institutional and country affiliations accurately. The extracted data was then cleaned to remove any duplicates and verify citation counts. Keywords were standardized to account for variations in terminology while maintaining conceptual integrity.

The bibliometric analysis employed three main analytical approaches. First, citation analysis was conducted to identify influential papers and authors within the field. Second, co-citation analysis was performed to map intellectual relationships between publications and identify key research clusters. Third, collaboration patterns were analyzed through author collaboration networks, with special attention to international research partnerships. These analyses were supported by network visualization techniques to map the relationships between authors, institutions, and research themes. The analysis particularly focused on identifying emerging research fronts and evolving patterns in the field of intelligence communication studies.

After conducting a comprehensive search of the existing literature, a bibliometric analysis was performed to map the intellectual structure of intelligence communication studies in the context of national security. The dataset for this research was obtained from major academic databases and included a wide range of publications related to intelligence communication and national security.

Bibliometric analysis involves using various statistical and visualization techniques to identify key themes, emerging trends, influential authors, and critical research areas within intelligence communication studies (Anwar et al., 2018). This approach allows for a systematic and objective examination of the scholarly landscape, providing valuable insights into the field’s evolution and current state of research (Wai, 2020).

Bibliometric analyses also facilitate the identification of potential gaps and opportunities for future research (Donthu et al., 2021), offering a foundation for academics and policymakers to make informed decisions and progress in the field of intelligence communications in the context of national security. The most prominent themes in the field of intelligence communications studies in the context of national security include the impact of technology on the collection and dissemination of intelligence information, the role of communications in intelligence operations, and ethical and legal considerations surrounding intelligence communications.

Results

Authorship Pattern and Country Distribution Analysis

This bibliometric study analyses the distribution of articles on national security and intelligence communications from different countries (Table 1). The available data show that the United States and the United Kingdom dominate in terms of the number of articles published and citations obtained. The US has 20 articles with a total of 80 citations, while the UK has 19 articles with 148 citations.

Australia and Canada are also significant contributors to this topic. Australia had 6 articles with 16 citations, while Canada had 5 articles with 37 citations. These countries play an important role in research related to national security and intelligence communications.

Meanwhile, some other countries, such as Brazil, South Korea, Ukraine, Belgium, China, Germany, Greece, India, Iran, Japan, Kuwait, Netherlands, New Zealand, Russia, Spain, Switzerland, Turkey, United Arab Emirates, and Zimbabwe have more limited contributions. Most of these countries have only one or two articles with relatively low citations.

Overall, this bibliometric analysis illustrates that the United States, the United Kingdom, Australia, and Canada lead the way regarding article publications and citations related to national security and intelligence communications. Meanwhile, contributions from other countries appear to be more limited in this study.

Table 1 Distribution of articles by country

Country	Documents	Citations
United States	20	80
United Kingdom	19	148
Australia	6	16
Canada	5	37
Spain	3	3
Brazil	2	4
South Korea	2	2
Ukraine	2	10
Belgium	1	12
China	1	6
France	1	0
Germany	1	12
Greece	1	10
India	1	9
Iran	1	1
Japan	1	3
Kuwait	1	3
Netherlands	1	3
New Zealand	1	5
Russian Federation	1	11
Switzerland	1	0
Turkey	1	3
United Arab Emirates	1	3
Zimbabwe	1	3

The insights gained from bibliometric analyses have opened new avenues for research and exploration in the study of communication intelligence. One emerging area of interest is the intersection of intelligence communication with emerging technologies such as artificial intelligence and machine learning. Understanding how these technologies can enhance intelligence collection and analysis, as well as the implications for communication strategies in national security, provides exciting opportunities for further investigation.

Another promising research direction highlighted by this analysis is the examination of the role of social media and digital platforms in shaping public perceptions

and opinions regarding national security and intelligence matters (Langmia, 2023; Taylor, 2021; Whyte, 2020). This involves exploring the dynamics of information dissemination, the spread of disinformation and misinformation, and the influence of online communities on intelligence communications.

Citation and Co-Citation Analysis

Based on [Table 2](#), we can understand that national security and intelligence communications are a major concern in many recent studies. The most cited articles discuss the impact of Snowden's disclosures on journalists and their confidential sources. This shows that issues of mass surveillance and privacy are at the forefront of national security and intelligence.

In addition, the threat of terrorism, information warfare, and cyber-attacks were also important topics discussed in several articles. This reflects the incredible attention to potential security threats arising from cyberspace and the use of information technology for malicious purposes.

Several studies also focused on metadata and the broader impact of surveillance. This indicates that surveillance impacts not only individual privacy but can also have wider consequences for society and various sectors.

In addition, several articles addressed topics such as government access to private sector data, surveillance impact assessment, and the potential use of AI for malicious purposes. This reflects the growing concern about how technology can be utilised for nefarious purposes and the importance of developing methodologies to assess and manage surveillance impacts.

Overall, [Table 2](#) provides an overview of the complex knowledge structure and research trends in the field of national security and intelligence communications. Topics covered include issues such as privacy, mass surveillance, cyber threats, metadata, the broader impact

Table 2 Articles with more than 10 citations

Article	Citations
No More Sources?: The impact of Snowden's revelations on journalists and their confidential sources (Lashmar, 2017)	34
Affecting Trust: Terrorism, Internet and Offensive Information Warfare (Valeri & Knights, 2000)	17
Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage (Lindsay, 2020)	16
Tracing the traces: The critical role of metadata within networked communications (Mayernik & Acker, 2018)	16
Beyond privacy: Articulating the broader harms of pervasive mass surveillance (Parsons, 2015)	15
The right to privacy and the future of mass surveillance (Watt, 2017)	15
Security and Surveillance in Virtual Worlds: Who Is Watching the Warlocks and Why? (Stevens, 2015)	12
Developing and testing a surveillance impact assessment methodology (Wright et al., 2015)	12
Government access to private-sector data in the United Kingdom (Brown, 2012)	12
Malicious use of artificial intelligence: New psychological security risks in BRICS countries (Bazarkina & Pashentsev, 2020)	11
Metadata laws, journalism and resistance in Australia (Brevini, 2017)	11

of surveillance, and the role of information technology in the context of national security and intelligence.

The co-citation analysis identified several distinct intellectual clusters in the field (Figure 1):

(1) Privacy and Surveillance Studies cluster, dominated by works focusing on data protection and surveillance implications;

(2) Technological Impact cluster, centered on digital transformation and cybersecurity;

(3) Policy and Governance cluster, emphasizing regulatory frameworks and institutional approaches; and

(4) Operational Intelligence cluster, focusing on practical implementation and strategies.

Author collaboration patterns reveal increasing international cooperation, with strong ties particularly between US-UK institutions, and emerging collaboration networks with institutions in Asia and Europe.

Thematic and Keyword Network Analysis

Based on Figure 1, several main keywords are connected to the concepts of “national security” and “intelligence communications.” These keywords include intelligence, strategy, surveillance, service management, privacy, ownership, and artificial intelligence.

The center point of the graph shows the word “national security agency”, which is closely connected to the concepts of national security and intelligence communications. From there, a network is formed that

connects various related aspects such as intelligence, surveillance strategy, intelligence service management, data privacy, information ownership, and the role of artificial intelligence.

This visualization provides an overview of the scope and structure of knowledge in research related to national security and intelligence communications. The relationships between concepts show the interconnectedness of issues such as surveillance, data management, privacy, and the role of modern technology in intelligence activities to protect national security.

Bibliometric analysis with network visualization helps to map the research landscape, identify key topics, and see the relationships between concepts within a knowledge domain. This is useful for comprehensively understanding research structures and trends.

Key Findings

Bibliometric analysis with network visualization helps to map the research landscape, identify key topics, and see the relationships between concepts within a knowledge domain. This is useful for comprehensively understanding research structures and trends.

▪ Graph center: “National security agency” is the central point that is connected to almost all other concepts. This shows the crucial role of national security agencies in integrating various aspects related to security and intelligence.

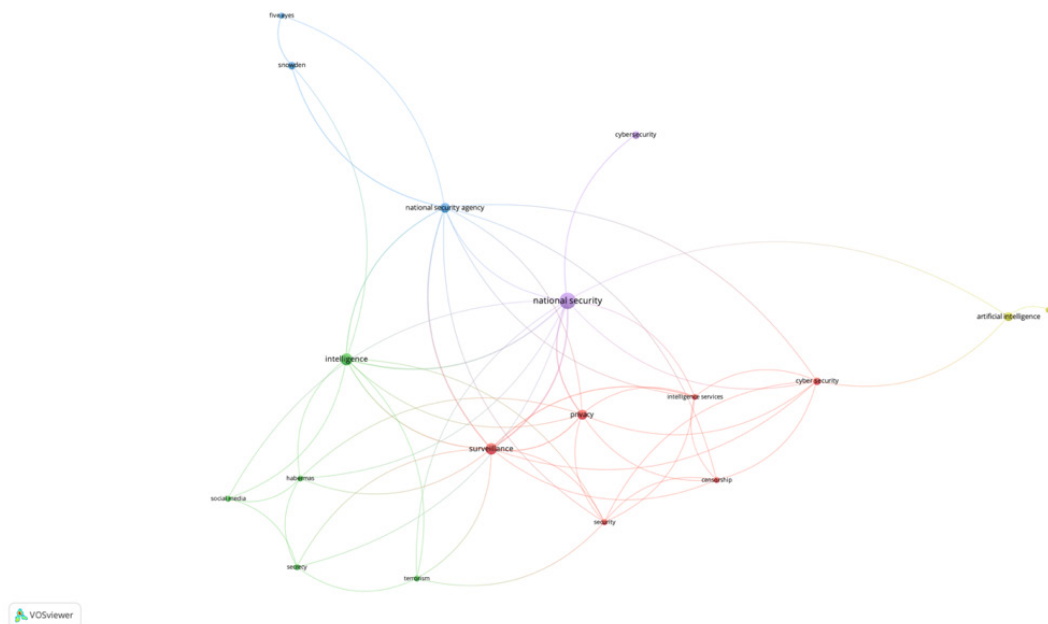


Figure 1 Visual occurrence analysis

- **Intelligence and Surveillance:** The concepts of “intelligence” and “surveillance” are closely related to “national security agency”. This reflects the importance of intelligence and surveillance activities in maintaining national security.

- **Strategy and Management Services:** The concepts of “strategy” and “intelligence services” are closely connected to national security. This indicates the importance of strategic planning and effective management of intelligence services.

- **Privacy and Ownership:** The concepts of “privacy” and “ownership” are connected to national security and intelligence. This suggests that there are considerations and debates regarding data privacy and information ownership in the context of national security.

- **Artificial Intelligence:** “Artificial intelligence” is connected to national security, hinting at the role of artificial intelligence technologies in modern intelligence operations and analyses.

- **Intelligence Communications:** Although not explicitly shown, “cyber security” can be associated with intelligence communications in the context of cybersecurity and information sharing.

Overall, this visualization illustrates the complexity and interconnectedness of various concepts in the national security and intelligence communications domains. These include technical aspects such as surveillance and intelligence, managerial aspects such as strategy and services, and social considerations such as privacy and data ownership. The role of cutting-edge technologies such as artificial intelligence is also integrated into this research landscape.

Discussion

Analysis of Research Patterns

The study titled “Mapping the Intellectual Structure of Intelligence Communication Studies in National Security Contexts: A Bibliometric Approach” delves into the realm of bibliometrics to analyze and map the intellectual landscape surrounding the intersection of national security and intelligence communication. Through the utilization of citation analysis, co-citation, and author collaboration, this research provides a comprehensive overview of the knowledge structure within this critical domain. The findings of the study reveal key themes and subtopics that have garnered significant attention, such as the impact of technology on intelligence information collection and dissemination, the role of communication

in intelligence operations, as well as the ethical and legal considerations surrounding intelligence communication. Furthermore, the research identifies significant patterns in author collaboration, indicating a trend towards interdisciplinary research and knowledge exchange.

The insights gleaned from this study shed light on the evolving nature of intelligence communication studies within national security contexts, emphasizing the growing importance of understanding how communication processes intersect with intelligence practices. By identifying central themes and emerging trends, the research contributes to a deeper understanding of the complexities inherent in intelligence communication and underscores the need for interdisciplinary collaboration to address contemporary challenges in this field. Moreover, the study’s focus on ethical and legal considerations surrounding intelligence communication highlights the nuanced ethical dilemmas and regulatory frameworks that shape the landscape of intelligence operations in the modern era.

Thematic Evolution and Trends

The emphasis on technological advancements and their impact on intelligence communication underscores the transformative role of technology in shaping the practices and methodologies employed in the field of national security. As information technologies continue to evolve rapidly, intelligence agencies are faced with both opportunities and challenges in harnessing these tools to enhance their operational capabilities while navigating the ethical and legal boundaries that govern information collection and dissemination. The study’s identification of key technological trends within intelligence communication studies provides valuable insights for policymakers, practitioners, and researchers seeking to navigate the complex terrain of modern intelligence operations.

Implications and Future Directions

The findings from this bibliometric analysis have significant theoretical and practical implications. Theoretically, this study advances our understanding of how intelligence communication research has evolved and identifies emerging frameworks in digital intelligence. Practically, these findings can inform policy development for intelligence agencies, particularly in areas of international collaboration and technological integration. Furthermore, the identified research gaps suggest opportunities for future studies in areas

such as artificial intelligence applications, cross-border intelligence sharing, and ethical frameworks for digital surveillance.

Furthermore, the study's exploration of author collaboration patterns highlights the increasing interconnectedness of researchers and practitioners across disciplinary boundaries. By fostering collaboration and knowledge exchange among experts from diverse fields, the study underscores the importance of interdisciplinary approaches in addressing the multifaceted challenges posed by intelligence communication in national security contexts. This collaborative ethos not only enriches the intellectual discourse within the field but also paves the way for innovative solutions that draw upon a diverse range of perspectives and expertise.

Conclusion

Conclude the research with discussion/reflections and recommendations based on the research findings. This bibliometric study uses a bibliometric approach to map the knowledge structure and research trends related to intelligence communications in the context of national security. By analyzing citations, co-citations, and author collaborations, the study provides insights into the main themes and subtopics that receive the most attention in this field.

Some of the critical themes identified include the impact of technology on intelligence collection and dissemination, the role of communications in intelligence operations, and ethical and legal considerations surrounding intelligence communications. In addition, the study also reveals patterns of author collaboration that demonstrate the trend of cross-disciplinary research and knowledge exchange between fields.

This study's main contribution is to provide a deeper understanding of the concepts, theories, and methodologies that shape the field of intelligence communications in the context of national security. By comprehensively mapping the research landscape, the findings emphasize the importance of cross-disciplinary collaboration in addressing the complexity of issues such as cybersecurity, the spread of disinformation, and the ethical implications of mass surveillance.

Furthermore, this bibliometric analysis also identifies opportunities for further research, such as the role of social media and digital platforms in shaping public perceptions of national security and the impact of artificial intelligence and machine learning on intelligence communications. The identification of these potential

research areas provides a roadmap for academics and practitioners to explore knowledge gaps and develop innovative solutions in the face of evolving national security challenges.

By summarising current knowledge and providing insights into future research directions, this study contributes to efforts to advance the field of intelligence communications and effectively safeguard national security. The study emphasizes the importance of cross-disciplinary collaboration in addressing the complexities of cybersecurity issues, the spread of disinformation, and the ethical implications of mass surveillance.

Overall, this bibliometric study provides an in-depth analysis of the scholarly structure of intelligence communication in national security and recommends future research directions to address increasingly complex and dynamic security challenges. The findings highlight the need for a holistic and multidisciplinary approach to understanding and addressing contemporary national security challenges. This section is not mandatory but can be added to the manuscript if the discussion is unusually long or complex.

Conflict of Interest

The authors declare that there is no conflict of interest.

References

- Anwar, M. A., Zhou, R., Wang, D., & Asmi, F. (2018). Mapping the knowledge of national security in the 21st century: A bibliometric study. *Cogent Social Sciences*, 4(1), 1542944. <https://doi.org/10.1080/023311886.2018.1542944>
- Bazarkina, D. Y., & Pashentsev, E. N. (2020). Malicious use of artificial intelligence. *Russia in Global Affairs*, 18(4), 154–177. <https://doi.org/10.31278/1810-6374-2020-18-4-154-177>
- Best, R. A. (2015). Intelligence and U.S. national security policy. *International Journal of Intelligence and CounterIntelligence*, 28(3), 449–467. <https://doi.org/10.1080/08850607.2015.1022460>
- Brevini, B. (2017). Metadata laws, journalism and resistance in Australia. *Media and Communication*, 5(1), 76–83. <https://doi.org/10.17645/mac.v5i1.810>
- Broniatowski, D. A. (2019). Communicating meaning in the intelligence enterprise. *Policy Insights from the Behavioral and Brain Sciences*, 6(1), 38–46. <https://doi.org/10.1177/2372732218792061>
- Brown, I. (2012). Government access to private-sector data in the United Kingdom. *International Data Privacy Law*, 2(4), 230–238. <https://doi.org/10.1093/idpl/ips018>
- Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2018). Intelligence and counterterrorism. In *Introduction to Homeland Security* (6th ed., pp. 121–143). Elsevier. <https://doi.org/10.1016/B978-0-12-804465-0.00005-4>
- Bury, P., & Chertoff, M. (2020). New intelligence strategies for a new decade. *The RUSI Journal*, 165(4), 42–53. <https://doi.org/10.1080/03071847.2020.1802945>

- Chen, B., Zhu, X., & Díaz del Castillo H., F. (2023). Integrating generative AI in knowledge building. *Computers and Education: Artificial Intelligence*, 5, 100184. <https://doi.org/10.1016/j.caeai.2023.100184>
- Cobley, P., & Schulz, P. J. (Eds.). (2013). *Theories and models of communication*: De Gruyter. <https://doi.org/10.1515/9783110240450>
- Degaut, M. (2016). Spies and policymakers: Intelligence in the information age. *Intelligence and National Security*, 31(4), 509–531. <https://doi.org/10.1080/02684527.2015.1017931>
- 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>
- Ellili, N. O. D. (2024). Bibliometric analysis of sustainability papers: Evidence from Environment, Development and sustainability. *Environment, Development and Sustainability*, 26(4), 8183–8209. <https://doi.org/10.1007/s10668-023-03067-6>
- Eriksson, G. (2018). A theoretical reframing of the intelligence–policy relation. *Intelligence and National Security*, 33(4), 553–561. <https://doi.org/10.1080/02684527.2018.1452558>
- Kammerer, K., Göster, M., Reichert, M., & Pryss, R. (2021). Ambalytics: A scalable and distributed system architecture concept for bibliometric network analyses. *Future Internet*, 13(8), 203. <https://doi.org/10.3390/fi13080203>
- Langmia, K. (Ed.). (2023). *Black communication in the age of disinformation: DeepFakes and synthetic media*. Springer. <https://doi.org/10.1007/978-3-031-27696-5>
- Lashmar, P. (2017). No more sources?: The impact of Snowden's revelations on journalists and their confidential sources. *Journalism Practice*, 11(6), 665–688. <https://doi.org/10.1080/17512786.2016.1179587>
- Lindsay, J. R. (2020). Demystifying the quantum threat: Infrastructure, institutions, and intelligence advantage. *Security Studies*, 29(2), 335–361. <https://doi.org/10.1080/09636412.2020.1722853>
- Mayernik, M. S., & Acker, A. (2018). Tracing the traces: The critical role of metadata within networked communications. *Journal of the Association for Information Science and Technology*, 69(1), 177–180. <https://doi.org/10.1002/asi.23927>
- Parsons, C. (2015). Beyond privacy: Articulating the broader harms of pervasive mass surveillance. *Media and Communication*, 3(3), 1–11. <https://doi.org/10.17645/mac.v3i3.263>
- Regens, J. L. (2019). Augmenting human cognition to enhance strategic, operational, and tactical intelligence. *Intelligence and National Security*, 34(5), 673–687. <https://doi.org/10.1080/02684527.2019.1579410>
- Stevens, T. (2015). Security and surveillance in virtual worlds: Who is watching the warlocks and why? *International Political Sociology*, 9(3), 230–247. <https://doi.org/10.1111/ips.12094>
- Taylor, B. C. (2021). Defending the state from digital deceit: The reflexive securitization of deepfake. *Critical Studies in Media Communication*, 38(1), 1–17. <https://doi.org/10.1080/15295036.2020.1833058>
- Tosun, N. (2018). Social networks as a learning and teaching environment and security in social networks. *Journal of Education and Training Studies*, 6(11a), 194. <https://doi.org/10.11114/jets.v6i11a.3817>
- Valeri, L., & Knights, M. (2000). Affecting trust: Terrorism, internet and offensive information warfare. *Terrorism and Political Violence*, 12(1), 15–36. <https://doi.org/10.1080/09546550008427547>
- Vogel, K. M., & Tyler, B. B. (2019). Interdisciplinary, cross-sector collaboration in the US intelligence community: Lessons learned from past and present efforts. *Intelligence and National Security*, 34(6), 851–880. <https://doi.org/10.1080/02684527.2019.1620545>
- Wai, J. (2020). Communicating intelligence research. *Journal of Intelligence*, 8(4), 40. <https://doi.org/10.3390/jintelligence8040040>
- Watt, E. (2017). The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, 21(7), 773–799. <https://doi.org/10.1080/13642987.2017.1298091>
- Whyte, C. (2020). Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. *Journal of Cyber Policy*, 5(2), 199–217. <https://doi.org/10.1080/23738871.2020.1797135>
- Willmetts, S. (2019). The cultural turn in intelligence studies. *Intelligence and National Security*, 34(6), 800–817. <https://doi.org/10.1080/02684527.2019.1615711>
- Wright, D., Friedewald, M., & Gellert, R. (2015). Developing and testing a surveillance impact assessment methodology. *International Data Privacy Law*, 5(1), 40–53. <https://doi.org/10.1093/idpl/ipu027>