Vol.5 Iss.6 2024
Communication & Education Review
https://doi.org/10.37420/j.cer.2024.085

Research on the Formation Mechanism of Disinformation in Intelligence Games

Ying Sun, Na Han*
People's Public Security University of China, Beijing, China
Corresponding author, E-mail:1092906562@qq.com

Abstract:
Disinformation, as an important tool in intelligence games, is used by countries as a hidden sword in political struggles, emerging as a new type of weapon in the context of the changing contemporary network environment and the intensifying competition among major powers. It has become a critical element of national security. Investigating the operational logic of disinformation in the digital era aims to help intelligence agencies prevent and mitigate disinformation crises and provide possible solutions for its governance. Based on the perspective of intelligence games, this paper summarizes the components of disinformation, analyzes the characteristics of disinformation in intelligence games, examines the internal logic of its formation in the digital era, and explores strategies for countering the threat posed by disinformation. Disinformation in the context of intelligence games is characterized by its global strategic nature, cognitive misdirection, and technological empowerment. As a special application in intelligence, disinformation follows a four-phase process: Plan, Do, Check, Act, from the generation of misleading content to the accurate dissemination of intelligence products. Based on this analysis, the paper proposes a Chinese strategy to actively confront the threat of disinformation.

Keywords:
Disinformation, Intelligence Games, National Security

1.Introduction

In 2022, with the outbreak of the "weaponization of information" during the Russia-Ukraine conflict, information manipulation gradually became a central theme in intelligence games during human warfare. "Disinformation," as a form of offensive counterintelligence through deception, has become one of the most common activities in the hybrid warfare space due to its low cost, fast dissemination, and wide-ranging impact. The term "disinformation" originates from the Russian intelligence agencies, where it was used to shape domestic and foreign public opinion and interfere with the policies and actions of foreign governments.

As the forms of warfare and communication technologies evolve, the production methods, dissemination channels, and influence of disinformation have constantly changed. Disinformation can be divided into three stages based on its dissemination medium: "print media - radio and television - smart media." In the print media era, disinformation, also known as "false intelligence," was primarily used in military fields, where false, incomplete, or misleading information was conveyed through newspapers or radio to target individuals, orga-

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

nizations, or countries to influence their intelligence judgment.

In the era of radio and television, disinformation extended beyond military tools to become an essential component of political and diplomatic strategies. During this period, Western countries defined disinformation as deliberately disseminating false information to deceive the public, manipulate public opinion, interfere in foreign domestic affairs, and disrupt social order. This was considered a key element of both information and psychological warfare.

In the era of smart media, intelligence games have gradually evolved into actions supported by reliable data, computational power, and algorithms. Data and algorithms not only control and alter the speed, nature, and direction of intelligence production but also enable the customized delivery of disinformation based on audience characteristics. Considering the developments brought by the convergence of information and intelligent technologies, this paper defines disinformation in national security intelligence games as the manipulation of intelligence to mislead, harm, or manipulate the audience, or create further divisions in existing conflicts to influence public perception, decision-making, or behavior.

Disinformation has a long history in strategic intelligence, closely linked to psychology, strategy, and national security. Existing research often focuses on the impact of disinformation on cybersecurity and military security from political or computer science perspectives. However, few studies systematically explore the principles, evolution, and operational mechanisms of disinformation from the perspective of intelligence games.

From a global perspective, disinformation has played a crucial role in significant events such as Brexit, color revolutions, and U.S. elections. It serves as a hidden weapon in political struggles and has been placed at the core of national security in an era of intensifying great power competition. In particular, Western countries, empowered by algorithms, have used disinformation to manipulate information in China, posing severe threats to national security. Unlike Western nations, China has not yet fully developed a comprehensive logic or defense system to counter disinformation.

This paper aims to deeply explore the mechanisms and strategies of disinformation manipulation, seeking effective interception and defense strategies. Therefore, in the face of new circumstances, we need to explore how disinformation functions within strategic deception. What is the interaction between national security, strategic deception, and disinformation? How does disinformation operate within the framework of strategic deception, and what risks does it pose to national security? To answer these questions, it is necessary to find answers from national security theory, strategic intelligence theory, and strategic information dissemination practices.

2.Constituent Elements of Disinformation

Disinformation, as a complex phenomenon of information manipulation, involves the deliberate fabrication and dissemination of false information, making the content of disinformation its core component. Disinformation is an intelligence game that involves both the manipulator (subject) and the target of deception (object). It is a multifaceted activity influenced by social culture, the knowledge background of both the manipulator

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

and the deceived party, and the context in which the event occurs. The rapid development of social media also provides important dissemination platforms for disinformation, increasing its influence and danger.

In summary, the primary elements of disinformation in the digital era include the subject, object, content, medium, and environment, as shown in Figure 1. These elements interact and together constitute the diversity of disinformation phenomena.

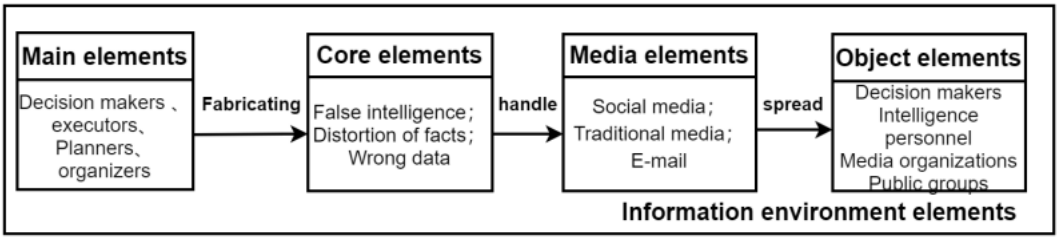


Figure 1: Components of Disinformation

1) Subject: The subject of disinformation refers to the party with an information advantage in the intelligence game, responsible for fabricating and disseminating deceptive information. They play different roles in the disinformation process, including decision-makers, implementers, planners, and organizers. The motivation and objectives of the manipulator play a crucial role in the formation and spread of disinformation. The goal is no longer limited to inducing the target to draw incorrect conclusions, but to mislead and distort the target's perception of facts through specific narrative techniques, thereby influencing the target's decisions.

2) Object: The object of disinformation refers to the target or audience receiving the deceptive information, who are passively influenced or harmed. Targets can include government decision-makers, intelligence analysts, media organizations, and the public. The success of disinformation often depends on the cognitive level, information sources, and sensitivity to false information of the object. Unlike other intelligence activities, the scope of disinformation is widespread and affects not only both parties in the intelligence game but also ordinary citizens, who are generally more susceptible to deception than intelligence analysts and decision-makers.

3) Content: The content of disinformation refers to the manipulated or altered information, which can include false news reports, distorted facts, erroneous statistical data, fabricated images, and videos. Disinformation content is typically misleading, deceptive, and manipulative, aimed at influencing the target's perception, attitude, and behavior.

4) Medium: The medium refers to the channels through which false information is disseminated, including emails, traditional media, and social media. With the development of digital technology, emerging platforms such as social media have become critical mediums for disinformation activities. These platforms' ability to quickly spread information and cover a broad audience makes them valuable tools for both sides of the intelligence game, significantly enhancing the reach and impact of disinformation.

5) Environment: The environment refers to the specific context in which disinformation is created and spread. It also includes the political climate, public opinion environment, and the openness and regulatory level of cyberspace. In the "post-truth" era, the complexity, plasticity, and instability of the information environment provide manipulators with favorable conditions for implementing disinformation.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

The interaction between these elements reflects the dynamic nature and uncertainty of disinformation activities. While content is the core element of disinformation, it can be utilized by both the manipulator and the target, demonstrating the dynamic intelligence game between the two sides.

3.Characteristics of Disinformation in Intelligence Games

3.1. Strategic Application: Global Strategic Nature

Disinformation, as a highly strategic intelligence tool, exhibits clear strategic directionality and profound influence at a macro level. In modern conflicts and great power rivalries, it plays an indispensable role. Its core function lies in supporting the achievement of strategic objectives through carefully crafted false information or misleading content, such as disrupting enemy decision-making processes, weakening their confidence, or even dismantling their alliances.

In the digital age, the global strategic nature of disinformation is characterized by "comprehensive, far-reaching, and deep." "Comprehensive" refers to the cross-domain deployment, as disinformation manipulations span multiple fields, requiring the manipulator to possess extensive knowledge and skills across various domains, integrating resources to formulate strategic goals. "Far-reaching" indicates that disinformation not only meets current tactical needs but also considers long-term challenges and opportunities to support broader strategic objectives. The ultimate goal is to ensure national security, safeguard national interests, and achieve national strategic goals. "Deep" means considering the long-term effects of disinformation. The results of intelligence activities, including disinformation, extend beyond a specific period or field and can have lasting impacts on a nation’s overall development and security.

3.2. Purpose of Intelligence: Cognitive Misdirection

The essence of disinformation lies in using information superiority to induce the opposing side to form erroneous perceptions and judgments. Misdirection is the primary purpose of disinformation and is a critical factor in the success of intelligence games. Disinformation is not a simple process of collecting, producing, and transmitting information but an adversarial activity aimed at misleading the opposing side’s cognition. By manipulating information as a weapon, the manipulator influences the enemy’s cognitive process, distorts their thinking, and ultimately impacts their decision-making. In the digital age, cognitive manipulation through disinformation no longer relies solely on the volume of false information but also leverages social and political divisions to mislead decision-makers. This can lead the target to make decisions that favor the manipulator without their awareness.

3.3. Intelligence Tools: Technological Empowerment

Technological empowerment is a unique characteristic of disinformation in the digital age, lowering the production cost of disinformation while increasing the complexity, adversarial nature, and unpredictability of intelligence activities. Currently, the technology behind disinformation involves artificial intelligence (AI), neuroscience, human enhancement, system integration, and adaptive algorithms. These emerging technologies have gradually enhanced the ability to produce false information, solidify cognitive biases, and enable

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

precise dissemination, introducing new intelligence adversarial capabilities.

4.The Formation Mechanism of Disinformation in the Digital Age

With the development of the digital age, the construction and dissemination of disinformation have also undergone changes. The generation of false information, the infiltration of dissemination technologies, and cognitive manipulation through neuroscience are intertwined, forming the internal generation logic of disinformation. The Deming Cycle (PDCA: Plan, Do, Check, Act) theory, a model for continuous quality improvement, has been widely used in decision-making processes and the evolution of intelligence applications. As a special form of intelligence, disinformation goes through four stages: Plan, Do, Check, and Act, from the generation of false information to its precise dissemination as an intelligence product. Based on the current state of artificial intelligence and communication studies, this paper structures a cyclical model of disinformation formation within the framework of intelligence games, as illustrated in Figure 2.

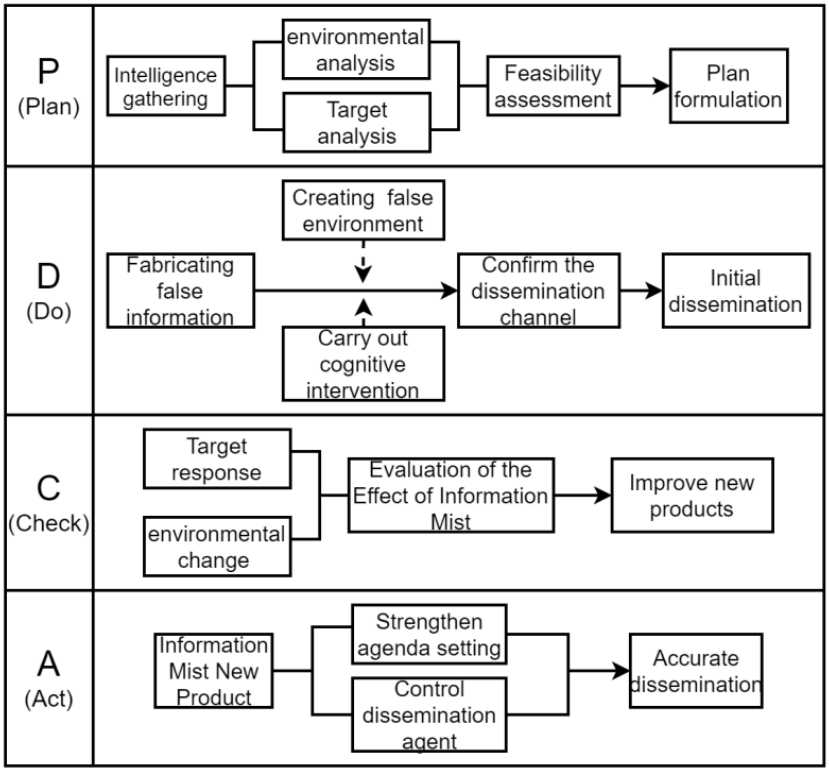


Figure 2: PDCA Cycle for the Construction of Disinformation in the Digital Age

4.1. Planning Stage: Comprehensive Assessment and Formulation of Disinformation Plans

In the planning stage, disinformation manipulators formulate specific objectives based on the overall intelligence strategy and specific environmental conditions. The plan serves as a blueprint for the overall design of disinformation activities, outlining the detailed script for its execution. Understanding the strategic situation and assessing strategic objectives are the foundation of disinformation activities, while identifying the target is essential for ensuring the success of disinformation.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

The formulation of intelligence strategy requires a comprehensive evaluation of both the manipulator's and the opponent's capabilities, as well as strategic objectives. The plan must consider various factors, including the intelligence capabilities of both sides, the information environment, and the battlefield situation, to ensure that the strategy is targeted, forward-looking, and feasible. Artificial intelligence (AI) and big data analytics provide strong support for the formulation of disinformation strategies, helping manipulators quickly and accurately gather and analyze intelligence, identify the actions and intentions of both sides, and provide scientific bases for strategic decision-making. Furthermore, technology can enhance the monitoring and tracing of disinformation activities, preventing information attacks and interference from opponents, and improving the efficiency of executing disinformation strategies.

4.2 Evaluating Strategic Goals and Tactics

Clear goal setting is crucial to the success of a disinformation plan. Goals include both strategic goals, such as influencing the enemy's decision-making and distracting their attention, and tactical goals, such as covering up one's actions and confusing the enemy's intelligence. Based on these goals, big data can be used to assess the opponent's intelligence weaknesses and craft deception stories that lead the enemy to make decisions advantageous to the manipulator. The strategy must also include organizing command, resource allocation, and execution of actions to ensure the successful implementation of the disinformation plan and achieve the desired outcomes.

1) Execution Stage: Fabrication of Information and Execution of Disinformation Activities

The execution of disinformation typically involves multiple factors and stages working together. With the rapid growth of the internet, the generation and dissemination of false information, as well as changes in the information environment, all influence the ultimate effectiveness of disinformation activities.

2) Narrative Strategy and Fabrication of False Information

The narrative strategy in the digital age involves selectively presenting information by fabricating fictional storylines and characters to manipulate the audience's emotions and perceptions, thereby achieving the dissemination of false information. The degree to which these narratives deviate from the truth varies, from simple removal of context to manipulation or alteration of existing content, to the fabrication of entirely fictitious deceptive stories. In intelligence games, both sides have great leeway to construct false narratives by distorting facts, reconstructing original information, and manipulating the emotions and attitudes of intelligence analysts. Artificial intelligence tools, such as generative AI, can be employed to create highly persuasive and emotionally charged narratives that capture the audience's attention.

3) Creating Consensus and Shaping the Information Environment

No intelligence activity occurs in isolation from its context. Disinformation, as a fierce contest in intelligence games, must be grounded in the actual situation of strategic confrontation. False information can only achieve deceptive effects within a specific context. In creating a false information environment, public opinion guidance and control over the narrative play a crucial role. By controlling mainstream media and social media platforms, the manipulator can create a false information environment, where fabricated consensus amplifies irrational opinions and influences public perceptions and behavior. This includes controlling the

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

channels and content of information dissemination, selecting appropriate topics and angles for reporting, and guiding public opinion to form unified views and attitudes.

4) Manipulating Cognitive Biases and Interfering with Intelligence Analysis

The human cognitive system plays a crucial role in processing and analyzing information. Cognitive psychology research has shown that people's cognitive systems are prone to various weaknesses and biases, which can be exploited in intelligence games to manipulate individual and group thinking and behavior. In the digital age, manipulators leverage emerging technologies like neuroscience to influence the cognitive system more covertly and precisely, guiding the audience into deepening their belief in the fabricated false information. In social media, for example, algorithmic recommendations can reinforce cognitive biases and stereotypes, while inducing anxiety and a sense of information scarcity, prompting people to accept specific viewpoints.

4.3. Evaluation Stage: Feedback and Adjustment

Disinformation is a continuously evolving process, requiring timely feedback on the opponent's reactions and changes in the information environment. Adjustments need to be made to the content and method of disseminating false information based on these dynamics.

1) Monitoring and Evaluating Target Reactions and Information Environment

Monitoring the target's reactions helps manipulators understand the emotional tendencies, focus points, and attitude changes of the audience toward the false information. It also aids both sides in intelligence games in identifying and responding to potential backlashes from disinformation activities. The manipulator must adapt to new changes in the information environment to ensure that the false information continues to be trusted by intelligence analysts.

2) Establishing a Feedback Mechanism to Improve Disinformation

Given the complexity and uncertainty of disinformation, feedback and adjustment are ongoing processes that require iteration and upgrades. The manipulator must choose the right timing for delivering false information, ideally when the opponent is in critical need of key intelligence but unable to thoroughly analyze it. In the dynamic implementation of disinformation, the content, dissemination channels, and methods need to be fine-tuned in response to changing contexts.

4.4. Action Stage: Technological Empowerment for Precise Dissemination

The action stage involves the actual dissemination of false information. With the rise of smart algorithms in social media platforms, strategic dissemination now takes the form of "precision distribution," targeting specific groups based on their preferences and behaviors.

1) Strengthening Agenda-Setting and Amplifying Public Opinion

Agenda-setting involves the selection and highlighting of specific topics to guide public attention and influence public perception. Manipulators use social media platforms to amplify the exposure of specific disinfor-

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

mation narratives by posting large volumes of content and leveraging comments, trending topics, and social media influencers to increase their impact. Through data analysis, manipulators can target specific audiences and design tailored agenda-setting strategies to reinforce the false information's influence.

2) Manipulating Proxy Dissemination and Polluting Communication Channels

Proxy dissemination involves using bots and other automated tools to spread fabricated information. These tools can quickly replicate and distribute pre-designed content across multiple channels, flooding the information space and generating artificial popularity. The repetitive nature of the content, combined with algorithmic amplification, pushes false narratives into public discourse, attracting further attention and lending credibility to disinformation.

5.Countermeasures Against Disinformation in Intelligence Games

5.1. Improving Top-Level Design: Balancing External Prevention and Internal Governance

In the new security environment, disinformation, empowered by digital technologies, poses an increasing threat to national security, social stability, and military security within the framework of national security intelligence games. Given China's national conditions, an intelligence strategy centered on disinformation should adopt a model led by national intelligence agencies with the participation of various stakeholders.

First, under the guidance of the concept of comprehensive national security, China should proactively build an active intelligence defense mechanism. National intelligence agencies should establish an overarching policy framework that clearly outlines the goals and strategies for managing false information. Facing the potential threats of national division and social unrest caused by disinformation, the government must exercise its sovereignty over cyberspace to mitigate security risks arising from digital development and maintain national security and social stability.

Second, it is essential to establish a nationwide intelligence-sharing system across intelligence domains to create a unified information management platform. This will facilitate the exchange of intelligence and the integration of resources, thereby enhancing the ability to respond to risks and improve decision-making efficiency.

Third, when developing external defense strategies, international cooperation should also be considered. In light of the fact that key information technologies and media resources are still dominated by Western countries, China should adopt defensive countermeasures to combat information manipulation by these countries. Understanding the mechanisms behind Western disinformation activities and developing effective countermeasures are crucial. Furthermore, China should strengthen its international cooperation by participating in high-level discussions on disinformation governance, advocating for the establishment of global standards, and contributing to the development of trusted AI technologies and risk management approaches.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

5.2. Enhancing Counterintelligence Capabilities and Improving Deception Detection

From the perspective of intelligence games, disinformation is a contest between the intelligence agencies of opposing sides. To successfully implement disinformation strategies, the manipulator must first understand the intelligence capabilities and cognitive level of the opposing side, as well as the information gap between them.

First, improving reconnaissance capabilities and balancing various intelligence-gathering methods are crucial to enhancing counterintelligence abilities. Intelligence agencies should continuously upgrade reconnaissance technologies, incorporating advanced surveillance equipment, remote sensing technologies, and other high-tech tools to improve the efficiency and quality of intelligence collection. Additionally, agencies should invest in both human and technical intelligence to ensure a balanced development of all intelligence domains, maximizing the effectiveness of intelligence gathering and analysis.

Second, adopting competitive intelligence analysis can help reduce errors in intelligence processing. Breaking the "filter bubble" is essential for detecting disinformation. By comparing and analyzing collected intelligence from multiple sources, intelligence analysts can distinguish between real and false information, thereby reducing the likelihood of deception.

Third, keeping pace with the development of new technologies on which disinformation relies is vital for deception detection. Disinformation increasingly depends on emerging technologies. Intelligence agencies should collaborate closely with research institutions and high-tech enterprises to develop key intelligence technologies, particularly those that enhance defenses against artificial intelligence risks. The development of privacy computing, algorithmic defense mechanisms, and deepfake detection technologies is crucial for improving network and information security. Monitoring AI-generated content will also help mitigate the impact of disinformation.

6.Conclusion

This study examines the phenomenon of disinformation within the context of intelligence games, building upon the PDCA cycle theory to develop a research framework. It reveals that the formation of disinformation involves a four-phase process: planning, constructing, evaluating, and acting. The paper clarifies the strategic and tactical implications of disinformation in the digital age, emphasizing the importance of technological empowerment.

In response to the threat posed by disinformation, China should actively explore countermeasures aligned with its national context. Guided by the concept of comprehensive national security, the country should address both internal and external risks, strengthening its defensive capabilities while ensuring a balanced development of intelligence competencies. By continuously improving its capacity to respond to intelligence threats, China can better safeguard its national security in the evolving landscape of information warfare.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

References

[1]Jones, A. (2012). The origins of disinformation in 20th century Russia. Journal of Political Propaganda, 15(3), 45-62.

[2]Bennett, W. L., & Livingston, S. (2023). A brief history of the disinformation age: Information wars and the decline of institutional authority. In Streamlining Political Communication Concepts (pp. 43-73). Springer International Publishing.

[3]Aïmeur, E., Amri, S., & Brassard, G. (2023). Fake news, disinformation, and misinformation in social media: A review. Social Network Analysis and Mining, 13(1), 30.

[4]Ji, D., Jiang, X., & Zhu, H. (2023). Theoretical innovation and practical exploration of computational communication. News and Writing, (12), 113.

[5]Guo, C., & Hou, Y. (2023). Research on the attack mechanism of information fog in social media. Journal of Information, 42(11), 113-118.

[6]Su, P., & Wang, Y. (2021). Intelligence observation on the fog of information: Concept, formation, and response. Theory and Practice of Intelligence, 44(03), 6-12.

[7]Wang, B., & Wu, C. (2021). Information fog: An important target in national strategic competition. Theory and Practice of Intelligence, 44(03), 13-18+68.

[8]Wang, H. (2022). The EU's actions in managing information fog and their significance. Library and Information, (01), 57-65.

[9]Konieczny, M. (2023). Ignorance, disinformation, manipulation, and hate speech as effective tools of political power. Policija i Sigurnost, 32(2), 123-134.

[10]Chang, J., & Luo, Y. (2023). How artificial intelligence "generates" information disorder: Principles, crises, and reflections. Information Technology and Management Applications, 2(03), 65-75.

[11]Bachmann, S. D., Putter, D., & Duczynski, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. Global Policy, 14(5), 858-869.

[12]Mirza, M. S., Begum, L., & Niu, L., et al. (2023). Tactics, threats & targets: Modeling disinformation and its mitigation. NDSS.

[13]Hui, L., & Barton, W. (2011). General discussion on strategic deception [C]. In Selected Translations on Strategic Deception and Surprise Attack (pp. 109-117). Military Yiwen Publishing House.

[14]Smith, J. (2020). Formulating effective information warfare strategies. International Journal of Intelligence, 25(3), 312-325.

[15]Feuerriegel, S., DiResta, R., & Goldstein, J. A., et al. (2023). Research can help to tackle AI-generated disinformation. Nature Human Behaviour, 7(11), 1818-1821.

[16]Bushell, S. (1992). Implementing plan do check and act. The Journal for Quality and Participation, 15(5), 58.

[17]Morris, L. (2018). Setting objectives for deception operations. International Journal of Intelligence, 23(4), 432-445.

[18]Davis, R. (2019). The role of media control in shaping public opinion. Journal of Media Studies, 45(2), 212-225.

[19]Karinshak, E., & Jin, Y. (2023). AI-driven disinformation: A framework for organizational preparation and response. Journal of Communication Management, 27(4), 539-562.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

[20]Han, N., & Dong, X. (2024). Cognitive domain security in the digital age: Theoretical deconstruction, risk generation, and governance pathways. International Security Studies, 42(03), 55-75+158-159.
[21]Tang, J., & Xing, C. (2023). Rumors as weapons: Cognitive manipulation based on computational propaganda. Journalism University, (08), 16-30+116-117.
[22]Zhao, W. (2024). Strengthening agenda-setting to enhance the effectiveness of public opinion guidance. Journalism Front, (07), 62-64.
[23]Murphy, B. J. (2023). In defense of disinformation. Journal of Homeland Security and Emergency Management.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)