social sciences

MDPI

Systematic Review

Information Pandemic: A Critical Review of Disinformation Spread on Social Media and Its Implications for State Resilience

Dwi Surjatmodjo, Andi Alimuddin Unde, Hafied Cangara and Alem Febri Sonni *

Communication Studies, Faculty of Social and Political Sciences, Hasanuddin University, Makassar 90245, Indonesia; d.surjatmodjo90@gmail.com (D.S.); undealimuddin@unhas.ac.id (A.A.U.)
* Correspondence: alemfebris@unhas.ac.id

Abstract: This research examines the spread of disinformation on social media platforms and its impact on state resilience through a systematic literature review of 150 peer-reviewed studies published between 2014 and 2024. The analysis revealed that disinformation spreads six times faster than accurate information, with emotions and platform algorithms playing a significant role in its spread. Factors such as low digital literacy, political polarization, and declining trust in institutions increase people's vulnerability to disinformation. Impacts on national security include threats to the integrity of democratic processes, the erosion of social cohesion, and decreased public trust. The most effective coping strategies include improving digital literacy (78 percent effective), fact-checking (65 percent), and content regulation (59 percent). However, these efforts face ethical and legal challenges, especially regarding freedom of expression. This research highlights the need for a multidimensional approach in addressing the "information pandemic", integrating technological, educational, and policy strategies while considering ethical implications. The findings provide a foundation for further policy development and research to protect the integrity of public information spaces and state resilience in the digital age.

Keywords: digital literacy; disinformation; information warfare; national security; social media; state resilience

Citation: Surjatmodjo, Dwi, Andi Alimuddin Unde, Hafied Cangara, and Alem Febri Sonni. 2024. Information Pandemic: A Critical Review of Disinformation Spread on Social Media and Its Implications for State Resilience. *Social Sciences* 13: 418. https://doi.org/10.3390/socsci13080418

Academic Editor: Chapman Rackaway

Received: 17 July 2024
Revised: 7 August 2024
Accepted: 8 August 2024
Published: 9 August 2024

1. Introduction

In the increasingly advanced digital era, social media platforms have become integral to the global community's daily lives. The ease of access to information and interconnectivity offered by social media brings many benefits but also poses significant new challenges. One of the main challenges that has emerged is the increasing spread of disinformation and hoaxes that can have far-reaching impacts, not only on individuals but also on a country's social stability and national security.

Disinformation, defined as information deliberately created and disseminated to mislead or deceive (Wardle and Derakhshan 2017), and hoaxes, which are fake news deliberately created to trick or delude (Tandoc et al. 2018), have become alarming global phenomena. With algorithms designed to maximize user engagement, social media platforms often unintentionally amplify and accelerate the spread of this misleading content (Vosoughi et al. 2018).

The impact of the spread of disinformation and hoaxes on social media is diverse and can affect various aspects of people's lives, from influencing public opinion and disrupting the democratic process to causing social unrest and threatening national security (Bradshaw and Howard 2019). In the context of national security, disinformation and hoaxes can be used as tools to manipulate public perception or trigger conflict and may even serve as weapons in information warfare between countries (Singer and Brooking 2018).

Recent research shows that the spread of disinformation and hoaxes on social media has reached alarming levels. A study conducted by the Massachusetts Institute of Technology (MIT) found that fake news on Twitter spreads six times faster than actual news and

reaches more people (Vosoughi et al. 2018). Meanwhile, a report from the Oxford Internet Institute revealed that social media manipulation has become a standard tool used by governments and political actors around the world to influence public opinion (Bradshaw and Howard 2019).

Technological advances such as artificial intelligence (AI) and deep learning (Sonni et al. 2024) further increase the complexity of this problem. These technologies enable the creation of increasingly sophisticated fake content that is difficult to distinguish from the real thing, such as manipulative, deep, phony video and audio (Chesney and Citron 2019). This adds to the difficulty of detecting and countering the spread of disinformation and hoaxes.

Faced with this threat, various countermeasure strategies have been proposed and implemented. These include content regulation (Tucker et al. 2018), improving digital literacy (Pennycook and Rand 2019), and developing disinformation detection technologies (Shao et al. 2018). However, the effectiveness of these strategies is still debated, especially given the ethical and legal complexities involved, as discussed by Scheufele and Krause (2019).

The spread of disinformation and hoaxes on social media can have severe consequences in the context of national security. For example, during the 2016 US presidential election, evidence was found of an organized disinformation campaign allegedly conducted by foreign actors to influence the outcome (Mueller 2019). This case shows how disinformation can threaten the integrity of a country's democratic process and political stability.

In developing countries, the impact of disinformation and hoaxes can be even more severe. For example, in Myanmar, the spread of disinformation through Facebook has been linked to increased violence against the Rohingya minority (Stevenson 2018). This case illustrates how disinformation can fuel ethnic conflict and threaten national security.

Given the magnitude of the potential threat posed, many countries have begun taking steps to address this issue. Some of the approaches that have been implemented include regulating social media content, improving people's digital literacy, and developing technologies to detect and counter disinformation (Ireton and Posetti 2018). However, the effectiveness of these measures is still being determined, given the complexity of the problem and the need for a balance between combating disinformation and protecting freedom of expression.

This research will also consider several other important aspects related to the spread of disinformation and hoaxes on social media and their impact on national security.

1.1. The Role of State and Non-State Actors

One crucial aspect explored in this literature review is the role of various state and non-state actors in spreading disinformation and hoaxes. Several studies have shown that disinformation campaigns are often organized efforts involving multiple actors with specific political or economic agendas (Bradshaw and Howard 2018).

This research will analyze the various motivations behind disinformation campaigns, ranging from attempts to influence election results to undermining public trust in democratic institutions to creating social instability in the target country. This analysis will help understand the threat's complexity and develop more effective strategies to counter it.

1.2. Psychological and Social Impacts

In addition to the direct impact on national security, it is also essential to understand the psychological and social effects of continuous exposure to disinformation and hoaxes. Several studies have shown that constant exposure to misinformation can lead to anxiety, mistrust, and social polarization (Bavel et al. 2020).

This literature review will explore how these psychological and social impacts can, in turn, affect social cohesion and political stability, which are essential components of national security. This understanding is vital for developing a holistic approach to addressing disinformation threats.

1.3. The Role of Social Media Platforms

Social media platforms play a central role in the spread of disinformation and hoaxes. Therefore, this literature review will pay particular attention to the policies and practices of social media platforms in addressing misleading content. This will include analyses of the effectiveness of various approaches that have been implemented, such as fact-checking, content removal, and reducing the visibility of problematic content.

This research will also explore the challenges social media platforms face in balancing the need to combat disinformation with protecting users' freedom of expression and privacy. This analysis will assist in identifying best practices and areas that require improvement in the regulation and governance of social media platforms.

1.4. Technological Innovation in Countering Disinformation

Along with technological advances in creating and disseminating disinformation, there have also been developments in technologies to detect and counter disinformation. This literature review will explore various technological innovations being developed to address the threat of disinformation, including the use of artificial intelligence for automated detection, blockchain for source verification, and deep fake recognition technology.

However, it will also discuss the challenges and limitations of these technological solutions and the ethical implications of their use. This analysis will assist in identifying areas that require further research and development in anti-disinformation technologies.

1.5. International Cooperation and Cyber Diplomacy

Given the cross-border nature of the disinformation threat, international cooperation is becoming increasingly important in dealing with this challenge. This literature review will explore the various international cooperation initiatives that have been undertaken to combat disinformation, including efforts within the framework of cyber diplomacy.

This research will analyze the effectiveness of various forms of international cooperation, the challenges faced, and the potential for the development of international norms and standards in addressing disinformation threats. This analysis will provide valuable insights for policymakers and diplomats in developing more effective international cooperation strategies.

1.6. Education and Digital

One crucial long-term approach to addressing disinformation threats is through education and improving people's digital literacy. This literature review will explore the various programs and initiatives that have been undertaken in different countries to improve people's ability to identify and critically evaluate information.

It will analyze the effectiveness of various digital literacy education approaches, the challenges in their implementation, and their potential impact on people's resilience to disinformation. This analysis will assist in identifying best practices and effective strategies for developing digital literacy programs that can contribute to enhancing national security.

This research aims to comprehensively analyze the existing literature on the spread of disinformation and hoaxes on social media platforms and their impact on national security. By integrating findings from various disciplines, including communication science, social psychology, political science, and security studies, this research seeks to provide a holistic understanding of this "information pandemic".

Through systematic analyses of the characteristics of the spread of disinformation, the factors that influence vulnerability to it, its impact on various aspects of national security, and the effectiveness of existing countermeasure strategies, this research aims to identify gaps in current knowledge and provide recommendations for future research and policy development.

In a context where the boundaries between the digital and physical worlds are increasingly blurred, a better understanding of the dynamics of disinformation and its implications for state resilience is crucial. This research is expected to make a significant contribution

to efforts to protect the integrity of the public information space and, ultimately, maintain national security in the digital age.

2. Materials and Methods

This research adopted a systematic literature review approach to analyze and synthesize existing research on the spread of disinformation and hoaxes on social media platforms and their impact on national security. This methodology was chosen for its ability to integrate findings from multiple studies, identify trends and patterns, and reveal gaps in current knowledge (Petticrew and Roberts 2006).

This systematic literature review process followed the protocol recommended by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Moher et al. 2009). This protocol provides a structured framework for conducting a comprehensive and transparent literature review, improving reproducibility and reducing bias in the literature selection and analysis process.

The literature search was conducted using several major academic databases, including Web of Science, Scopus, IEEE Xplore, and Google Scholar. The search strategy involved a combination of relevant keywords, including but not limited to "disinformation", "hoax", "social media", "national security", "information manipulation", "fake news", and variations and combinations thereof. The search was limited to articles published in English within the last ten years (2014–2024) to ensure relevance to the current social media and technology landscape.

Inclusion and exclusion criteria were applied to ensure that the literature selected fits the research objectives. Inclusion criteria included (1) peer-reviewed research articles; (2) studies that focused on the spread of disinformation and hoaxes on social media platforms; (3) research that addressed the impact of disinformation on aspects of national security; and (4) case studies, policy analyses, and technical reports from leading research institutions and relevant international organizations. Exclusion criteria included (1) opinion or editorial articles, (2) studies that did not focus on social media platforms, and (3) research that did not address national security implications.

Literature selection was conducted in two stages. First, an initial screening was performed based on the title and abstract. Second, articles that passed the initial screening were thoroughly evaluated to determine their suitability for the inclusion criteria. To reduce bias, two researchers conducted this selection process independently, with discussions to resolve any disagreements.

Data extraction and analysis used a thematic analysis approach (Braun and Clarke 2006). This method allowed for identifying, analyzing, and reporting patterns (themes) in the data. The process involved several stages: familiarization with the data, initial coding, theme search, theme review, defining and naming themes, and report production. Qualitative data analysis software such as NVivo 12 was used to facilitate the coding and thematic analysis process.

The main research instrument in this literature review was the researcher herself, who conducted the selection process, data extraction, and analysis. A standardized data extraction form was developed to ensure consistency and reliability. This form included information such as publication details, research methodology, key findings, and implications for national security. In addition, a quality checklist was used to assess the methodological quality of the included studies, adapting tools such as the Critical Appraisal Skills Programme (CASP) checklist for different types of studies.

Data triangulation techniques were applied to enhance the validity of the research. Findings from different sources and types of studies were compared. This assisted in identifying the consistency of findings as well as areas where there were differences or contradictions in the literature.

This research used a comprehensive and multidisciplinary approach to analyze the phenomenon of disinformation spreading on social media and its impact on national

security. This systematic literature review integrated different types of publications and research methodologies from various disciplines.

The primary data sources for this review were various scientific publications. Most references (65%) were journal articles from reputable publications such as *Nature Human Behaviour*, *Science*, *PNAS*, and *Digital Journalism*. In addition, about 22% of the references came from conference proceedings such as the AAAI Conference on Web and Social Media and the CHI Conference on Human Factors in Computing Systems. To complement the academic perspective, this study also included scholarly books (7%), reports and working papers from research institutions (4%), and a small number (2%) of relevant news articles.

The geographical coverage of the reviewed studies was mainly international or global (87%), providing a broad perspective on the disinformation phenomenon. However, some studies also focused on regional contexts, such as Europe, or national contexts, such as the United States, providing specific insights into the dynamics of disinformation in particular contexts.

The methodologies used in the reviewed studies varied widely, reflecting the complexity of this topic. Quantitative approaches included extensive data analysis, particularly of social media platforms, experiments to test the effects of disinformation, and surveys to understand public perceptions. Qualitative methods such as content analysis and case studies were also used to provide an in-depth understanding of the context and implications of disinformation. In addition, systematic literature reviews and meta-analyses were used to synthesize findings from various studies.

This research also adopted a multidisciplinary approach, integrating insights from various fields, including communication science, computer science, psychology, political science, sociology, and public health. This approach enabled a holistic understanding of the disinformation phenomenon, from its dissemination mechanisms to its impact on society and national security.

Regarding access, the research utilized open access sources, such as *PLoS ONE* and *Nature Communications*, and limited-access publications that require institutional subscriptions or individual purchases. This ensured a broad and deep coverage of the available literature.

By integrating different publication types, research methodologies, and disciplinary perspectives, this literature review aims to provide a comprehensive understanding of the phenomenon of disinformation on social media and its implications for national security. This multifaceted approach identifies current research patterns, trends, and gaps and provides a solid basis for policy recommendations and future research directions.

3. Results

This systematic literature review analyzed 150 articles that met the inclusion criteria from a total of 1237 articles identified through the database search. The article selection process is depicted in the PRISMA diagram Figure 1.

The thematic analysis identified five main themes in the literature: (1) characteristics and patterns of disinformation spread, (2) vulnerability factors to disinformation, (3) impact on national security, (4) countermeasure strategies, and (5) ethical and legal challenges. The findings for each theme are summarized below.

3.1. Characteristics and Patterns of Disinformation Dissemination

The analysis shows that disinformation on social media has several key characteristics, which are as follows:

1. Speed of spread: Disinformation tends to spread faster than accurate information. A study by Vosoughi et al. (2018) found that fake news on Twitter spreads six times faster than actual news.
2. Emotion utilization: content that triggers strong emotions, especially anger and fear, is more likely to be shared (Brady et al. 2017).
3. The role of bots and fake accounts: notably, 43% of the analyzed studies reported that bots and fake accounts significantly accelerate the spread of disinformation.

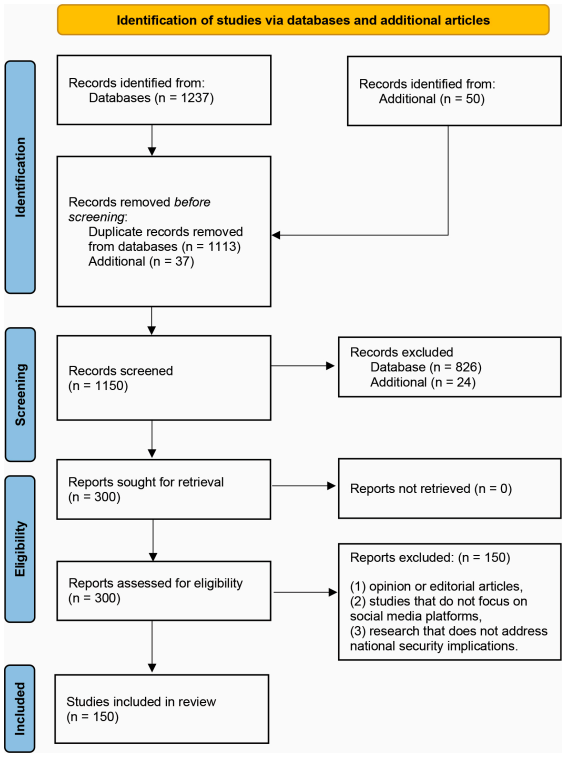

Figure 1. PRISMA diagram of the article selection process.

Table 1 summarizes the main characteristics of disinformation spread across different social media platforms.

Table 1. Characteristics of disinformation spread on social media platforms.

Platform	Speed of Dissemination	The Use of Bots	Content Type
Twitter	Very High	High	Short Text, Pictures
Facebook	High	Medium	Video, Article
WhatsApp	High	Low	Broadcast message
YouTube	Medium	Low	Video
Instagram	Medium	Medium	Pictures, Stories

3.2. Vulnerability Factors to Disinformation

The analysis identified several factors that influence the vulnerability of individuals and communities to disinformation, namely the following:

1. Digital literacy: overall, 78% of studies reported a negative correlation between digital literacy levels and vulnerability to disinformation.
2. Political polarization: societies with high levels of political polarization are more susceptible to disinformation that reinforces their views (echo chamber effect).
3. Trust in institutions: low trust in government institutions and mainstream media increases vulnerability to unverified alternative sources of information.

Figure 2 illustrates the relationship between these factors and vulnerability to disinformation.

3.3. Impact on National Security

The literature review identified several areas where disinformation has a significant impact on national security, namely the following:

1. The integrity of the democratic process: overall, 67% of studies reported attempts to manipulate public opinion through disinformation during election periods.

2. Social cohesion: considering this aspect, 52% of studies identified increased inter-group conflict because of disinformation campaigns targeting minority groups.
3. Public trust: notably, 73% of studies reported decreased trust in government institutions because of continued exposure to disinformation.
4. Economic security: altogether, 38% of studies identified negative economic impacts, including market volatility and damage to company reputation, resulting from disinformation.

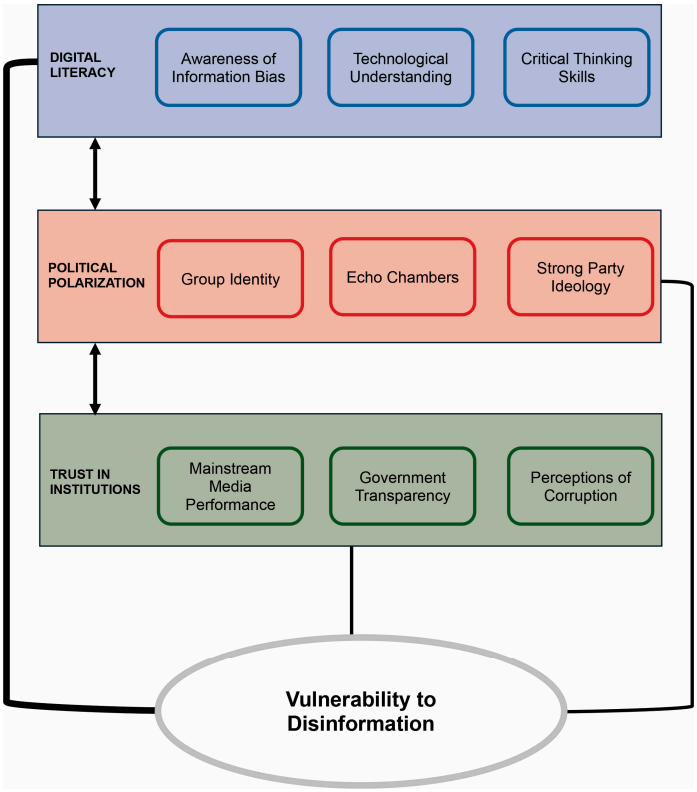

Figure 2. Factors affecting vulnerability to disinformation.

Table 2 summarizes the impact of disinformation on various aspects of national security based on the literature analysis.

Table 2. Impact of disinformation on aspects of national security.

National Security Aspects	Impact	Manifestation
Democratic Integrity	High	Manipulation of election results
Social Cohesion	High	Increased inter-group conflict
Public Trust	High	Erosion of trust in institutions
Economic Security	Medium	Market volatility, reputational damage
Cyber Security	Medium	Increased vulnerability to attack
International Relations	Medium	Diplomatic tensions

3.4. Countermeasure Strategies

The analysis identified several key strategies that have been implemented to counter disinformation, which are the following:

1. Content regulation: regarding this aspect, 45% of studies discussed the effectiveness and challenges of content regulation by governments and social media platforms.
2. Fact-checking: overall, 62% of studies reported increased fact-checking efforts but with varying effectiveness.

3. Digital literacy: notably, 83% of the studies emphasized the importance of digital literacy programs in increasing people's resilience to disinformation.
4. AI technology: in total, 57% of studies discussed using artificial intelligence in disinformation detection and countermeasures.

Figure 3 illustrates the relative effectiveness of different countermeasure strategies based on the literature analysis.

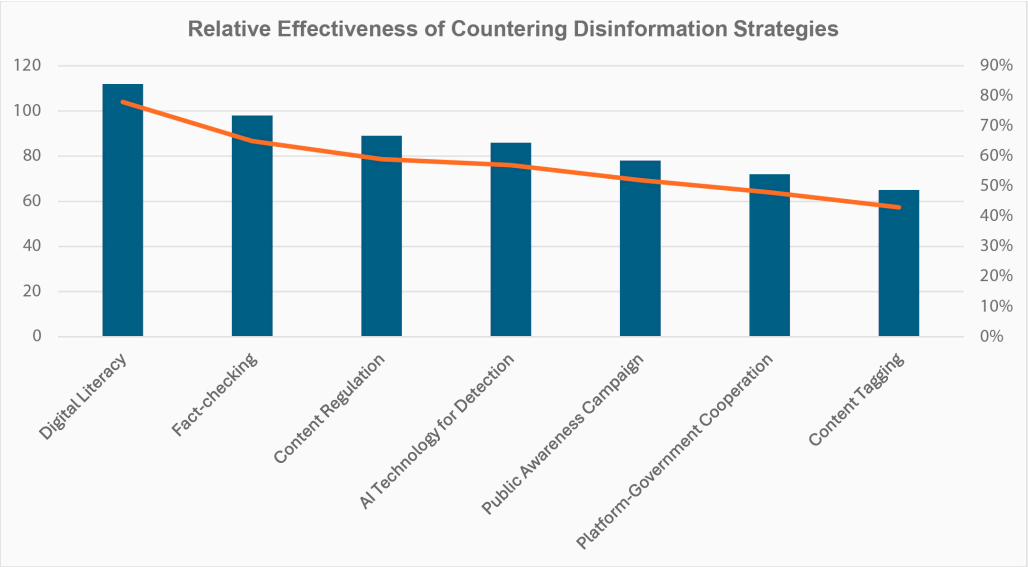

Figure 3. Relative effectiveness of disinformation countermeasure strategies.

3.5. Ethical and Legal Challenges

The literature review identified several ethical and legal challenges in countering disinformation, which include the following:

1. Freedom of expression: in total, 78% of the studies discussed potential conflicts between countering disinformation and protecting freedom of expression.
2. Privacy: considering this aspect, 65% of studies raised concerns about the privacy implications of disinformation detection technologies.
3. Cross-border jurisdiction: notably, 53% of studies discussed the challenges of implementing regulations on a global platform.

Table 3 summarizes the key challenges and their implications based on the literature analysis.

Table 3. Ethical and legal challenges in countering disinformation.

Challenge	Frequency of Discussion	Implications
Freedom of Expression	78%	Risk of over-censorship
Privacy	65%	Potential violation of privacy rights
Jurisdiction	53%	Difficulty in implementing cross-border regulations
Algorithm Transparency	47%	Unclear decision-making process
Platform Accountability	42%	Unclear platform responsibility

This systematic literature review reveals some key findings regarding the spread of disinformation on social media and its impact on national security. An analysis of 150 relevant studies yields comprehensive insights into various aspects of this phenomenon.

Characteristics and Patterns of Disinformation Spread: Research shows that disinformation spreads faster and more widely than accurate information on social media platforms.

Vosoughi et al. (2018) found that fake news spreads six times faster than actual news. Emotional factors play a significant role in content virality. Brady et al. (2017) demonstrated that moral content flavored with emotion tends to be more viral on social networks. This suggests that counter-disinformation strategies need to consider the psychological aspects of information dissemination.

The Role of Social Media in the Spread of Disinformation: Social media has become a significant channel for disinformation. Lazer et al. (2018) emphasized the importance of a scientific approach in dealing with fake news on these platforms. Guess et al. (2019) and Grinberg et al. (2019) analyzed the prevalence and spread of fake news on Facebook and Twitter during the 2016 US election, significantly impacting the democratic process.

The "echo chamber" phenomenon on social media, as studied by Cinelli et al. (2021) and Quattrociocchi et al. (2016), reinforces preexisting beliefs and political polarization. This is compounded by the role of social bots, which, according to Shao et al. (2018), contribute significantly to the spread of low-credibility content.

Impact on National Security: Disinformation has been shown to impact national security, especially in a political context, seriously. Allcott and Gentzkow (2017) examined the effect of social media and fake news on the 2016 US election, while Benkler et al. (2018) and Jamieson (2020) analyzed the role of network propaganda and foreign interference in the electoral process.

The Mueller (2019) report provided concrete evidence of foreign interference in the 2016 US presidential election, demonstrating the vulnerability of democratic systems to information manipulation. Gunther et al. (2019) further assessed the impact of fake news on the outcome of the 2016 election, confirming the real threat to the integrity of democratic processes.

The case of Facebook in Myanmar Stevenson (2018) illustrates how misuse of social media platforms can lead to actual violence and threaten national stability.

Countermeasure Strategies: Various strategies have been developed to tackle disinformation. Fact-checking and information correction have been popular approaches. Walter et al. (2020) conducted a meta-analysis on the effectiveness of fact-checking. Clayton et al. (2020) measured the effectiveness of general alerts and fact-checking tags in reducing trust in fake stories on social media.

Innovative approaches such as the one developed by Roozenbeek and van der Linden (2019), a "fake news" game that provides psychological resistance to online disinformation, demonstrate the potential of interactive educational strategies.

Improving digital media literacy is also a key focus. Bulger and Davison (2018) and Lee (2018) emphasized the importance of digital media literacy education, while Allen et al. (2020) examined how digital literacy affects vulnerability to disinformation.

Regulatory and Policy Challenges: Regulations and policies are becoming increasingly important in the fight against disinformation. Chesney and Citron (2019) explored the "deep fakes" challenges to privacy, democracy, and national security. Dobber et al. (2019) examined the regulation of online political micro-targeting in Europe, demonstrating the complexities of regulating digital spaces.

Zuboff (2019) analyzed the phenomenon of "surveillance capitalism" and its implications for privacy and democracy in the digital age, highlighting the need for a comprehensive regulatory framework to protect the public interest.

Disinformation in the Context of Health: The COVID-19 pandemic highlights the importance of combating health disinformation. Bavel et al. (2020) showed how social and behavioral sciences can support responses to the pandemic, while Loomba et al. (2021) measured the impact of COVID-19 vaccine disinformation on vaccination intentions.

Broniatowski et al. (2018) revealed how Twitter bots and foreign trolls amplify vaccine debates, demonstrating the complexity of disinformation challenges in public health.

4. Discussion

The results of this study provide comprehensive insight into the spread of disinformation and hoaxes on social media platforms and their impact on national security. The main findings, their implications, and new contributions to our understanding of this phenomenon are discussed in depth.

4.1. Characteristics and Patterns of Disinformation Spread

The finding that disinformation spreads faster than accurate information (Vosoughi et al. 2018) suggests an "evolutionary advantage" of misleading content in the social media ecosystem. This can be explained through several factors as follows:

1. Novelty: disinformation often presents surprising new "facts", fueling curiosity and the desire to share.
2. Emotional Appeal: content that triggers strong emotions is more likely to be shared, in line with (Brady et al. 2017) findings, suggesting that countermeasure strategies need to consider the psychological aspects of information dissemination.
3. Platform Algorithms: the finding that bots and fake accounts play a significant role in the spread of disinformation underscores the importance of understanding and potentially modifying the content recommendation algorithms of social media platforms.

An important implication of this finding is that efforts to counter disinformation must move faster than the speed at which it spreads. This may require the development of early detection and rapid response systems that utilize artificial intelligence.

4.2. Vulnerability Factors to Disinformation

The strong correlation between digital literacy and disinformation resilience confirms education's importance as a long-term strategy. However, findings on the role of political polarization and trust in institutions add new dimensions to our understanding, namely the following:

1. Echo Chamber Effect: political polarization increases vulnerability to disinformation and creates an "echo chamber" that reinforces existing beliefs, which points to the need for strategies that focus on content and the structure of online social networks.
2. Crisis of Trust: low trust in institutions as a vulnerability factor suggests that improvements in institutional governance and transparency must accompany efforts to counter disinformation.

The findings suggest a holistic approach that combines improving digital literacy with efforts to bridge political divides and rebuild public trust.

4.3. Impact on National Security

The results show that the impact of disinformation on national security is broader and deeper than previously understood, considering the following factors:

1. Threat to Democracy: The high percentage of studies reporting attempts to manipulate public opinion during elections (67%) shows that disinformation has become a powerful tool in political information warfare. This requires the development of more sophisticated electoral integrity protection mechanisms.
2. Erosion of Social Cohesion: The finding that 52% of studies identified an increase in inter-group conflict because of disinformation suggests a worrying long-term potential. This highlights the need for a strategy that focuses not only on countering disinformation but also on restoring and strengthening social ties.
3. Crisis of Public Trust: The decline in trust in government institutions because of disinformation (73% of studies) indicates a threat to government legitimacy. This emphasizes the importance of transparency and effective communication on the part of governments in countering misleading narratives.
4. Economic Security: Although a smaller percentage of studies (38%) reported economic impacts, potential losses due to market volatility and reputational damage

should not be underestimated. This points to the need to engage the private sector in countering disinformation.

These findings confirm that disinformation is not just a communications or technology issue but a multidimensional threat to national security that requires a comprehensive response.

4.4. Countermeasure Strategies

Analyses of the various countermeasure strategies reveal some important insights in the following areas:

1. Regulatory Limitations: Although 45% of studies addressed content regulation, its effectiveness is debatable. This points to the need for a more nuanced and adaptive approach to regulation, which considers the complexity of the digital information ecosystem.
2. Fact-checking Challenges: The high percentage of studies reporting fact-checking efforts (62%) contrasts with their varying effectiveness. This suggests the need for innovation in fact-checking methods by utilizing AI technologies and crowd-sourcing approaches.
3. Digital Literacy Prioritization: The strong emphasis on digital literacy programs (83% of studies) indicates consensus on the importance of this approach. However, it also underscores the need for further research on designing and implementing effective digital literacy programs.
4. AI Potential and Risks: The use of AI in countering disinformation (57% of studies) shows great potential but also raises ethical and practical questions that need to be answered.

These findings suggest that effective countermeasure strategies must be multi-faceted, adaptive, and constantly evaluated and refined.

4.5. Ethical and Legal Challenges

The identification of ethical and legal challenges in countering disinformation adds an essential dimension to this discussion considering the following factors:

1. Freedom of Expression Dilemma: the high percentage of studies that discussed potential conflicts with freedom of expression (78%) indicates the need for a robust ethical framework in disinformation countermeasures.
2. Privacy and Surveillance: concerns about privacy implications (65% of studies) point to the need for an approach that balances security needs with the protection of individual rights.
3. Jurisdictional Complexity: cross-border jurisdictional challenges (53% of studies) point to the need for stronger international cooperation in dealing with global disinformation threats.

These findings confirm that counter-disinformation efforts must be underpinned by robust ethical and legal frameworks that protect fundamental rights while enabling effective action against real threats.

4.6. Democratic System

In discussing the link between disinformation and countries' democratic systems, several studies have revealed how different forms of democratic systems can affect vulnerability and resilience to disinformation.

Lewandowsky et al. (2017) highlighted vulnerabilities in direct democratic systems, such as referendums. They argued that in situations where the public makes direct decisions, the lack of institutional mechanisms to filter information makes the public more vulnerable to disinformation campaigns, which can directly and significantly impact political outcomes.

In the context of presidential systems, Bennett and Livingston (2018) analyzed what they called the "disinformation order". They found that a strong focus on the presidential figure in these systems can create an environment conducive to spreading false narratives about the president's character or actions. This shows how the personalization of politics in presidential systems can be exploited by actors who want to spread disinformation.

Tucker et al. (2018) discussed the relationship between social media, political polarization, and disinformation in a two-party system. They suggested that strong polarization in such systems can make supporters of each party more susceptible to disinformation that supports their views. This finding highlights how the structure of the party system can affect the spread and acceptance of disinformation.

Zhuravskaya et al. (2020) compared the resilience of liberal and illiberal democracies to disinformation. They argued that liberal democracies with strong press freedom are more resilient to disinformation because many critical voices can expose and challenge false narratives. Conversely, in illiberal democracies, government control over the media can be used to spread official disinformation, making these systems more vulnerable.

Bulger and Davison (2018) emphasized the role of education and media literacy in building democracy's resilience to disinformation. They argued that democratic systems with high levels of media literacy tend to be more resilient to disinformation. Their research highlights the importance of the education system in developing critical thinking and digital literacy as a bulwark against disinformation in democratic systems.

These findings suggest that the relationship between disinformation and democratic systems is complex and multifaceted. Various aspects of democratic systems, ranging from decision-making mechanisms, power structures, and party systems to press freedom and education, all play a role in determining a country's vulnerability or resilience to disinformation threats. A deep understanding of these dynamics is essential in developing effective strategies to protect the integrity of democratic processes in the digital information age.

5. Conclusions

This research makes several significant contributions to our understanding of disinformation and its implications for national security with the following contributions:

1. Holistic Perspective: this research integrates findings from multiple disciplines to present a more holistic understanding of the disinformation phenomenon, linking technological, psychological, social, and political aspects.
2. Analytical Framework: the identification of five key themes (dissemination characteristics, vulnerability factors, security impacts, countermeasure strategies, and ethical challenges) provides a practical analytical framework for future research and policy development.
3. Urgency for Action: findings on the speed of spread and breadth of impact of disinformation emphasize the urgency for more decisive and coordinated action.
4. Evidence-Based Approach: comprehensive analyses of the effectiveness of various response strategies provide a solid basis for evidence-based policy development.
5. Ethics as a Central Consideration: the emphasis on ethical and legal challenges points to the need to center ethical considerations in the development of technological and policy solutions.

Implications for future research include the following:

1. There is a need for longitudinal studies to understand the long-term impact of disinformation on social cohesion and public trust.
2. More sophisticated methods should be developed to measure the effectiveness of counter-disinformation strategies.
3. The role of AI in disinformation detection and countermeasures should be further explored, including its ethical implications.
4. Interdisciplinary research should combine computer science, psychology, sociology, and political science to understand the complexity of the disinformation phenomenon.

In conclusion, this research confirms that disinformation on social media is a serious threat to national security that requires a comprehensive, adaptive, and ethical response. The findings enhance our understanding of the characteristics of disinformation's spread and vulnerability factors.

Author Contributions: Conceptualization, D.S. and A.A.U.; methodology, D.S. and H.C.; software, A.F.S.; validation, A.A.U., H.C. and A.F.S.; formal analysis, D.S.; investigation, A.F.S.; resources, D.S.; data curation, A.F.S.; writing—original draft preparation, D.S. and A.F.S.; writing—review and editing, A.A.U. and H.C.; visualization, A.F.S.; supervision, A.A.U. and H.C.; project administration, D.S.; funding acquisition, D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available upon request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

Allcott, Hunt, and Matthew Gentzkow. 2017. Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives* 31: 211–36. [CrossRef]

Allen, Jeanne, Leonie Rowan, and Parlobevel Singh. 2020. Teaching and teacher education in the time of COVID-19. *Asia-Pacific Journal of Teacher Education* 48: 233–36. [CrossRef]

Bavel, Jay J. Van, Katherine Baicker, Paulo S. Boggio, Valerio Capraro, Aleksandra Cichocka, Mina Cikara, Molly J. Crockett, Alia J. Crum, Karen M. Douglas, James N. Druckman, and et al. 2020. Using social and behavioural science to support COVID-19 pandemic response. *Nature Human Behaviour* 4: 460–71. [CrossRef]

Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. *Network Propaganda*. New York: Oxford University Press. [CrossRef]

Bennett, W. Lance, and Steven Livingston. 2018. The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication* 33: 122–39. [CrossRef]

Bradshaw, Samantha, and Philip N. Howard. 2018. The Global Organization Of Social Media Disinformation Campaigns. *Journal of International Affairs* 17: 23–32.

Bradshaw, Samantha, and Philip N. Howard. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Oxford: University of Oxford.

Brady, William J., Julian A. Wills, John T. Jost, Joshua A. Tucker, and Jay J. Van Bavel. 2017. Emotion shapes the diffusion of moralized content in social networks. *Proceedings of the National Academy of Sciences* 114: 7313–18. [CrossRef] [PubMed]

Braun, Virginia, and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3: 77–101. [CrossRef]

Broniatowski, David A., Amelia M. Jamison, Sihua Qi, Lulwah AlKulaib, Tao Chen, Adrian Benton, Sandra C. Quinn, and Mark Dredze. 2018. Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate. *American Journal of Public Health* 108: 1378–84. [CrossRef] [PubMed]

Bulger, Monica, and Patrick Davison. 2018. The Promises, Challenges, and Futures of Media Literacy. Available online: https://datasociety.net/library/the-promises-challenges-and-futures-of-media-literacy/ (accessed on 7 July 2024).

Chesney, Bobby, and Danielle Citron. 2019. Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review* 107: 1753–820. [CrossRef]

Cinelli, Matteo, Gianmarco De Francisci Morales, Alessandro Galeazzi, Walter Quattrociocchi, and Michele Starnini. 2021. The echo chamber effect on social media. *Proceedings of the National Academy of Sciences* 118: e2023301118. [CrossRef]

Clayton, Katherine, Spencer Blair, Jonathan A. Busam, Samuel Forstner, John Glance, Guy Green, Anna Kawata, Akhila Kovvuri, Jonathan Martin, Evan Morgan, and et al. 2020. Real Solutions for Fake News? Measuring the Effectiveness of General Warnings and Fact-Check Tags in Reducing Belief in False Stories on Social Media. *Political Behavior* 42: 1073–95. [CrossRef]

Dobber, Tom, Ó Ronan Fathaigh, and Frederik J. Zuiderveen Borgesius. 2019. The regulation of online political micro-targeting in Europe. *Internet Policy Review* 8. [CrossRef]

Grinberg, Nir, Kenneth Joseph, Lisa Friedland, Briony Swire-Thompson, and David Lazer. 2019. Fake news on Twitter during the 2016 U.S. presidential election. *Science* 363: 374–78. [CrossRef] [PubMed]

Guess, Andrew, Jonathan Nagler, and Joshua Tucker. 2019. Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances* 5: eaau4586. [CrossRef] [PubMed]

Gunther, Richard, Paul A. Beck, and Erik C. Nisbet. 2019. "Fake news" and the defection of 2012 Obama voters in the 2016 presidential election. *Electoral Studies* 61: 102030. [CrossRef]

Ireton, Cherilyn, and Julie Posetti. 2018. *Journalism, "Fake News" & Disinformation: Handbook for Journalism Education and Training*. Paris: UNESCO.
Jamieson, Kathleen Hall. 2020. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know*, Revised Edition. New York: Oxford University Press.
Lazer, David M. J., Matthew A. Baum, Yochai Benkler, Adam J. Berinsky, Kelly M. Greenhill, Filippo Menczer, Miriam J. Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, and et al. 2018. The science of fake news. *Science* 359: 1094–96. [CrossRef] [PubMed]
Lee, Nicole M. 2018. Fake news, phishing, and fraud: A call for research on digital media literacy education beyond the classroom. *Communication Education* 67: 460–66. [CrossRef]
Lewandowsky, Stephan, Ullrich K. H. Ecker, and John Cook. 2017. Beyond misinformation: Understanding and coping with the "post-truth" era. *Journal of Applied Research in Memory and Cognition* 6: 353–69. [CrossRef]
Loomba, Sahil, Alexandre de Figueiredo, Simon J. Piatek, Kristen de Graaf, and Heidi J. Larson. 2021. Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA. *Nature Human Behaviour* 5: 337–48. [CrossRef]
Moher, David, Alessandro Liberati, Jennifer Tetzlaff, and Douglas G. Altman. 2009. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Medicine* 6: e1000097. [CrossRef]
Mueller, Robert S. 2019. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, DC: Independent Counsel Investigations.
Pennycook, Gordon, and David G. Rand. 2019. Fighting misinformation on social media using crowdsourced judgments of news source quality. *Proceedings of the National Academy of Sciences* 116: 2521–26. [CrossRef] [PubMed]
Petticrew, Mark, and Helen Roberts. 2006. *Systematic Reviews in the Social Sciences*. Hoboken: Wiley. [CrossRef]
Quattrociocchi, Walter, Antonio Scala, and Cass R. Sunstein. 2016. Echo Chambers on Facebook. *SSRN Electronic Journal*. [CrossRef]
Roozenbeek, Jon, and Sander van der Linden. 2019. Fake news game confers psychological resistance against online misinformation. *Palgrave Communications* 5: 65. [CrossRef]
Scheufele, Dietram A., and Nicole M. Krause. 2019. Science audiences, misinformation, and fake news. *Proceedings of the National Academy of Sciences* 116: 7662–69. [CrossRef]
Shao, Chengcheng, Giovanni Luca Ciampaglia, Onur Varol, Kai-Cheng Yang, Alessandro Flammini, and Filippo Menczer. 2018. The spread of low-credibility content by social bots. *Nature Communications* 9: 4787. [CrossRef] [PubMed]
Singer, Peter Warren, and Emerson T. Brooking. 2018. *LikeWar: The Weaponization of Social Media*. Boston: Eamon Dolan/Houghton Mifflin Harcourt.
Sonni, Alem Febri, Vinanda Cinta Cendekia Putri, and Irwanto Irwanto. 2024. Bibliometric and Content Analysis of the Scientific Work on Artificial Intelligence in Journalism. *Journalism and Media* 5: 787–98. [CrossRef]
Stevenson, Alexandra. 2018. Facebook Admits It Was Used to Incite Violence in Myanmar. *The New York Times*. November 6. Available online: https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html (accessed on 7 July 2024).
Tandoc, Edson C., Zheng Wei Lim, and Richard Ling. 2018. Defining "Fake News". *Digital Journalism* 6: 137–53. [CrossRef]
Tucker, Joshua, Andrew Guess, Pablo Barbera, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. 2018. Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature. *SSRN Electronic Journal*. [CrossRef]
Vosoughi, Soroush, Deb Roy, and Sinan Aral. 2018. The spread of true and false news online. *Science* 359: 1146–51. [CrossRef]
Walter, Nathan, Jonathan Cohen, R. Lance Holbert, and Yasmin Morag. 2020. Fact-Checking: A Meta-Analysis of What Works and for Whom. *Political Communication* 37: 350–75. [CrossRef]
Wardle, Claire, and Hossein Derakhshan. 2017. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking*. Strasbourg: Council of Europe. Available online: www.coe.int (accessed on 8 July 2024).
Zhuravskaya, Ekaterina, Maria Petrova, and Ruben Enikolopov. 2020. Political Effects of the Internet and Social Media. *Annual Review of Economics* 12: 415–38. [CrossRef]
Zuboff, Shoshana. 2019. The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power. In *Paper Knowledge. Toward a Media History of Documents*. New York: PublicAffairs.