MISINFORMATION AND NATIONAL SECURITY: AN INTEGRATED FRAMEWORK FOR THREAT ANALYSIS AND INSTITUTIONAL RESILIENCE[1]

AHMED SHEHATA [1]

[1] Sultan Qaboos University, a.shehata@squ.edu.om

ABSTRACT Misinformation, a type of fake news, spreads via traditional and modern media channels, intentionally or unintentionally threatening individuals, organizations, and countries. This study aims to develop an integrated framework for analyzing misinformation threats and building institutional resilience while examining the effectiveness of various national approaches to countering misinformation. Through systematic content analysis of literature from 2015-2024, the research examines institutional responses across multiple nations, revealing significant variation in resilience levels based on media market structure, political polarization, and public trust. The resulting Institutional Resilience Framework Against Misinformation (IRFM) incorporates four key components: Structural Resilience Index, Educational Capacity Score, Response Mechanism Rating, and Societal Trust Quotient. Findings indicate that countries with regulated media environments, strong democratic institutions, and high media literacy demonstrate greater resilience to misinformation threats. The framework provides measurable metrics for assessing institutional vulnerability and building comprehensive defense mechanisms against evolving misinformation challenges while acknowledging implementation challenges in highly polarized environments.

INDEX TERMS Misinformation; Institutional Resilience; Media Literacy; National Security; Information Literacy.

المعلومات المضللة والأمن الوطني: إطار متكامل لتحليل التهديدات وبناء الصمود المؤسسي

أحمد الشحاته[1]

[1] جامعة السلطان قابوس، a.shehata@squ.edu.om

المستخلص تُعدّ المعلومات المضللة، وهي نوع من الأخبار الزائفة، ظاهرة تنتشر عبر وسائل الإعلام التقليدية والحديثة، بشكل متعمد أو غير متعمد، مما يشكّل تهديدًا للأفراد والمؤسسات والدول. تهدف هذه الدراسة إلى تطوير إطار متكامل لتحليل تهديدات المعلومات المضللة وبناء القدرة المؤسسية على الصمود، مع استقصاء فعالية النُهُج الوطنية المختلفة في التصدي لهذه الظاهرة. ومن خلال تحليل محتوى منهجي للأدبيات العلمية الممتدة بين عامي 2015 و2024، تستعرض الدراسة الاستجابات المؤسسية في عدد من الدول، كاشفة عن تباين ملحوظ في مستويات الصمود تبعًا لهيكل السوق الإعلامي، والاستقطاب السياسي، ومستويات الثقة العامة. ويقدّم إطار "القدرة المؤسسية على الصمود في مواجهة المعلومات المضللة" (IRFM) أربع مكونات رئيسية: مؤشر الصمود البنيوي، مقياس القدرات التعليمية، تصنيف آليات الاستجابة، ومُعامل الثقة المجتمعية. وتشير النتائج إلى أن الدول التي تتمتع ببيئات إعلامية منظمة، ومؤسسات ديمقراطية قوية، ومستويات عالية من الثقافة الإعلامية تُظهر قدرة أعلى على مواجهة تهديدات المعلومات المضللة. ويوفّر الإطار مؤشرات قابلة للقياس لتقييم هشاشة المؤسسات وبناء آليات دفاعية شاملة في مواجهة التحديات المتطورة، مع الاعتراف بصعوبة تطبيق هذه الآليات في البيئات ذات الاستقطاب الحاد.

الكلمات المفتاحية المعلومات المضللة؛ الصمود المؤسسي؛ الثقافة الإعلامية؛ الأمن الوطني؛ الثقافة المعلوماتية.

1. INTRODUCTION

Introduction to your research. (Background, importance, objectives). Misinformation presents a complex challenge in contemporary information ecosystems, with significant implications for national security, institutional stability, and social cohesion. While its historical roots trace back to the Cold War era when governments strategically deployed false information for geopolitical advantage, modern technological advancement and artificial intelligence have dramatically amplified its reach and impact (Monteith et al., 2023). Studies indicate that over 60% of social media users share content without verifying the original source, creating fertile ground for the rapid proliferation of false narratives (Cassar, 2023).

AHMED SHEHATA: MISINFORMATION AND NATIONAL SECURITY: AN INTEGRATED FRAMEWORK FOR THREAT ANALYSIS AND INSTITUTIONAL RESILIENCE

(JSDS)

The scope of national security concerns has expanded beyond traditional military and espionage threats to encompass information warfare and digital manipulation. Current research demonstrates how targeted misinformation campaigns can systematically erode public trust in institutions, influence electoral processes, and destabilize public health responses during crises like COVID-19 (Dumitrache & Popa, 2022). The impact varies significantly across different democratic contexts, with countries demonstrating varying levels of resilience based on their media ecosystems, political polarization, and institutional frameworks (Humprecht et al., 2020).

Cross-national studies reveal that institutional resilience to misinformation varies significantly based on several key factors: media market structure, political polarization, and public trust in mainstream institutions. Northern and Western European countries generally demonstrate higher resilience due to robust welfare systems and well-regulated media environments. In contrast, nations with higher political polarization and weaker mainstream media show increased vulnerability (Dragomir et al., 2024). These variations underscore the need for context-specific approaches to building institutional resilience.

The interdisciplinary nature of misinformation research spans information science, sociology, political science, and security studies. Despite the growing understanding of individual aspects, gaps remain in synthesizing these insights into actionable frameworks for institutional response. This study addresses this need by developing an integrated framework for analyzing misinformation threats and building institutional resilience, with particular attention to the role of education systems in fostering critical thinking and media literacy.

Through systematic content analysis of existing literature and empirical studies, this research aims to understand how misinformation operates within national security contexts comprehensively. By examining various national approaches to misinformation resilience, from regulatory frameworks like the EU's Code of Practice on Disinformation to educational initiatives in media literacy, the study seeks to identify effective strategies for institutional response and adaptation in an increasingly complex information environment.

2. STUDY OBJECTIVES

The primary objectives of this research are:

1. Develop an integrated analytical framework for assessing institutional vulnerabilities to misinformation threats in national security contexts.

2. Evaluate the effectiveness of different national approaches to building institutional resilience against misinformation, focusing on regulatory frameworks, educational initiatives, and media literacy programs.

3. Identify key factors contributing to institutional resilience across different contexts, particularly examining the relationship between media market structure, political polarization, and public trust.

4. Propose actionable strategies for strengthening institutional defense mechanisms against evolving misinformation challenges, with particular attention to the role of multi-stakeholder coordination and community engagement.

These objectives address the growing need for systematic approaches to understanding and countering misinformation threats while acknowledging the complex interplay between institutional structures, societal trust, and technological advancement.

3. RESEARCH QUESTIONS

This study This study addresses the following key research questions:

1. What are the primary mechanisms through which misinformation threatens institutional stability and national security across different democratic contexts?

2. How do variations in media market structure, political polarization, and public trust influence institutional resilience to misinformation threats?

3. What factors contribute to successful institutional responses to misinformation, as evidenced by cross-national comparative analysis?

4. How can educational initiatives and media literacy programs effectively contribute to building institutional resilience against misinformation?

5. What role do multi-stakeholder coordination and community engagement play in strengthening institutional defense mechanisms against evolving misinformation challenges?

4. LITERATURE REVIEW

The literature on misinformation and institutional resilience spans multiple disciplines and theoretical frameworks, reflecting the complex nature of contemporary information threats. This review examines two key areas: the evolving landscape of misinformation concerning national security and institutional approaches to building resilience against information threats. Recent scholarship has highlighted the transformation of misinformation from traditional propaganda to AI-enhanced digital manipulation, while

AHMED SHEHATA: MISINFORMATION AND NATIONAL SECURITY: AN INTEGRATED FRAMEWORK FOR THREAT ANALYSIS AND INSTITUTIONAL RESILIENCE

(JSDS)

simultaneously exploring varied institutional responses across different national contexts. This literature synthesis reveals the persistent challenges in combating misinformation and emerging frameworks for institutional adaptation and response. Understanding these parallel developments is crucial for developing effective countermeasures and building robust institutional defenses against evolving information threats.

5. MISINFORMATION AND NATIONAL SECURITY

The accelerated advancement in information technology has been alarming. Online platforms and the myriad media applications have altered the information environment. While such advancement and prevalence of information has been globally accepted as convenient and instantaneous, it has conveyed a new threat of fake, inaccurate, and illegitimate information or news. They have introduced new actors to the media market and opened access to individuals or groups who previously were marginalized and in need of revamping. Thus, the emerging problem of untrusted informational flow has reshaped and affected societies, institutions, and individuals as well.

Though the term misinformation or fake news may sound new, it goes back to the 1960s during World War II and the Cold War in Europe. Governments spread fake news to manipulate the war stream and create an impact on nations to maintain their geopolitical and economic stability. Law (2023) explained that in the 1950s, the US CIA (Central Intelligence Agency) purposely spread fake news about Guatemalan President Arbenz to oust him. They depicted their action as being "brilliant" as it aligned with their agenda of fighting the global spread of communism, claiming to maintain the US economic stability (cited in Ferreira, 2008). In the new technological era of AI (Artificial Intelligence), fake news or misinformation has been easily created and spread.

Cassar (2023) explained that with the AI implementation, illegitimate fake news has been harbored on websites and spread widely among people. The research revealed that (60.1%) of the participants share content from social media rather than the main source, which raises a red flag on the legitimacy of the information being shared. The absence of the fact-checking process and the repetitive exposure to such manipulation encourage people to believe in the content read or seen unconsciously. Englmeier (2021) explained that misinformation can range from fake news, lies, predictions, harmful truths, and pseudoscientific statements to unintentionally wrong statements, personal opinions, or misconceptions. Press channels and news may

have contributed to such dilemma when they lose their trustworthiness information sources and add their stance as parts of their reports.

Misinformation can cause mistrust among societies and deter cohesion by hampering reciprocal respect and esteem (Lo Sardo et al., 2024; Sultan & Zaman, 2023). Covid-19 can be a good example of information speculation and truth-finding struggle. It aroused fear, uncertainty, and anxiety among people worldwide. The lack of reciprocal trust can breed the ground for conspiracy theories. "People losing trust in reliable sources of information may become susceptible to conspiracy theories" (Englmeier, 2021). The implausible and sensational information can undermine people's confidence in journalism. Thus, fact-checking aligning with people's beliefs and knowledge can help in distinguishing falsehood from truth. Daunt et al. (2023) justified that individual psychology and social identity, as individuals drive self-esteem and belonging sensations from groups, are more likely to be either susceptible to fake news or more resilient. He argued that fake political news contains conspiratorial elements that aim to generate partisan tension or a sense of patriotism or even threaten the freedom of individuals by playing on ideological beliefs. Therefore, individuals are more likely to trust news that is affiliated with their identity and beliefs while rejecting other deviant news.

Calvillo et al. (2021) believed that fake news had a persistent presence on social media during the US (2016) presidential election. He assumed that political news has played a significant role in influencing public opinion on vital issues like health care and climate change. Such exposure to fake news could contribute to public distrust of mainstream media. On the other hand, individuals who are more conscientious and open-minded are more likely to discern fake news from accurate ones so easily. It is worth mentioning that financial markets and brand marketing have been affected by fake news through different forms of scams and fraud. It backed the existence of specialized websites that consist of a combination of credible yet distorted coverage of financial research and geopolitical news, which detriment price action and business in general (Cassar, 2023).

Belova & Georgieva (2018) claimed that business websites can agitate public opinion and provoke separation when state-sponsored misinformation. It can create the impression of supporting a specific candidate or idea domestically or broadly. Business news can produce a mix of genuine or sensational content when motivated to influence. Belova & Georgieva (2018) expressed concerns

AHMED SHEHATA: MISINFORMATION AND NATIONAL SECURITY: AN INTEGRATED FRAMEWORK FOR THREAT ANALYSIS AND INSTITUTIONAL RESILIENCE

(JSDS)

that such techniques have been used for political campaigns and can distribute malware. It was found that exposure to online misinformation was associated with lower trust in mainstream media (Ognyanova et al., 2020). They examined how exposure to misinformation can erode public confidence in social institutions. They revealed that public consumption of fake news has changed their attitude toward social institutions. Scholars, politicians, and journalists are concerned that such digestion of misinformation can destabilize political institutions and undermine mainstream media organizations in exigent circumstances when people require a reliable and trusted source of information. The consequence of such attitudes and behaviors can make the public more vulnerable to fake news by shifting trust from one political entity to another and from mainstream institutions to radical groups.

Ognyanova et al. (2020) concluded that "fake news was linked to a decrease in political trust among liberal respondents, but it is associated with an increase in political trust for moderates and conservatives." Accurate information shall diminish any other source of misperception and fake news when provided in a clear compelling format and by a trusted media source. Nyhan & Reifler (2019) asserted that the way information is displayed can affect people's perception of news. They claimed that when people encounter accurate information formatted in a way that can be easily counter-argument, it can lead to misperception. Thus, misperception can be caused by the lack of corrective information and psychological threats. News media has been characterized by systemic biases when deploying news in a dramatized or sensationalized fashion making them more pursued by the audience (Harcup & O'neill, 2017).

A cross-country survey was conducted by Van et al. (2024) across many democracies (the United States, the United Kingdom, the Netherlands, Germany, France, Poland, and India) to overview how the audience perceives the quality of news concerning the prevalence of misinformation and negativity bias. Though the finding revealed that negativity bias is more systematic and pervasive in news, misinformation alarms the audience as a disruptive threat across the surveyed countries. The study demonstrated that in countries where polarization is high and press freedom is low more concerns arise about negativity bias and misinformation. While in countries where an independent press can act freely without envisioned polarization concerns are relatively low. According to Serrano-Puche et al., 2023 in some countries where polarized and distrusted contexts are relatively high (e.g., the United States and

India), misinformation threat is perceived to be more alarming than where media is perceived to be trusted most of the time (e.g., Germany and the Netherlands).

Lee (2019) believed that most fake news revolves around politics and flourishes more in political climates, leading eventually to the spreading of misinformation on social media platforms. It has diminished the credibility of mainstream networks, portraying credibility to fake news. Adeyemi & Maria (2022) explained that a country like Nigeria (endures security challenges) used to rely on mainstream media as a trusted, reliable source of information. Before the emergence of social media, democracy in Nigeria thrived admirably due to the well-structured, carefully scrutinized reports. However, the political climate has witnessed a dynamic alteration after social media influencers sought self-promotion to gain more followers by spreading fake news. Spreading fake news among the public may cause social panic and generate turmoil threatening Nigeria's peace and tranquility.

Colliander (2019) examined the effect of exposure to social media users' comments on changing individual responses and attitudes toward posted information. He noticed the use of disclaimers on social media notifying users of the information authenticity has an irrelevant backwash on individuals' attitudes and propensity to make positive comments and intentions to share fake news. Nonetheless, a noticeable change in individuals' attitudes and propensity to share fake news was noted after the exposure to others' comments critical of fake news. Conversely, Wardle & Derakhshan (2017) believed that "Social networks are driven by the sharing of emotional content." Thus, they cannot be viewed as neutral communication pipelines since people tend to share posts and information that appeal to the prevailing attitude within their social circle.

The impact of misinformation dissemination can segregate societies into different races, religions, classes, politics, etc., invoking the collapse of welfare and democratic institutions. The disruption of misinformation during the pandemic of Corona Virus deployed social pressure on state decision-makers while trying to manage the pandemic. People doubted the efficiency of the vaccine believing in the conspiracy theory of its harmful effect on human health, disrespecting the rules countries sought to control the virus (Dumitrache & Popa, 2022). Challenging the security goals and objectives during critical times can negatively affect public health provoking harmful behavior and resistance to expert advice.

The interactive nature of online platforms and social media opened access to share information (both accurate and

AHMED SHEHATA: MISINFORMATION AND NATIONAL SECURITY: AN INTEGRATED FRAMEWORK FOR THREAT ANALYSIS AND INSTITUTIONAL RESILIENCE

(JSDS)

falsehood), which serves to shape public perception positively or negatively. The algorithms of such media contributed to prioritizing content that promotes sensational or controversial information (Firdaus et al., 2024). Studying how people cope with misinformation and understanding the antecedent conditions (applying the Recognition and Response Model (MRRM)) can help people develop effective responses and intervene properly against misinformation (Amazeen, 2024). Though it depends on individual traits and conceptual understanding, it may help to mitigate the implications of misinformation and generate personal and social mediation regarding media information. The velocity of information flood either on websites or social media is proliferated. Thus, people's perception of news reliability or distrust depends on how they consume and respond to news. Therefore, spreading awareness and building trust in mainstream media are indispensable to diminish misinformation and avoid eroding public confidence in social institutions.

6. INSTITUTION RESILIENCE TO MISINFORMATION THREAT

The proliferated flow of misinformation has manifested its presence in all societies all over the world. To avoid the impact of misinformation, community involvement is required to build and strengthen institutional resilience. Thus, the effort made by governments, industries, scholars, and communities to ease the impact of disseminating misinformation is perpetually challenged due to the dynamic of online information.

In January 2018, the European Commission (EC) launched the Code of Practice on Disinformation (COP) to tackle online disinformation. Facebook, Google, Twitter, Mozilla, and other advertising industry companies signed up for the newly drafted EU (COP). It was the first cross-Europe initiative to manage the challenges posed by the omnipresence of misinformation, disinformation, and fake news. It was revised in 2021 and signed by 34 signatories and presented in 2022. All signatories are aware of the fundamental right of individual freedom of speech, expression, and privacy. Accordingly, drawing a balance between individual fundamental rights and taking effective actions against the dissemination of misinformation is very critical. The signatories shall bid to build a fair and honest representation of their intentions. They shall commit and collaborate to ensure that the advertising industry bars the placement of harmful disinformation campaigns. Notwithstanding, Pamment (2022) argued that the expected strong trust had not been built between the government, industry, academia, and civil society. Some stakeholders

were viewed from the perspective of lobbying and manipulating public policy. He recommended stakeholders to work collaboratively and transparently on similar challenging areas based on mutual trust to help find and share effective solutions to encountering misinformation. The self-assessment approach of the COP should be backed with another form of regulatory intervention derived from the Democracy Action Plan (DSA) (Pamment, 2022).

In essence, such action would help improve oversight and set minimum standards for actors beyond signatories, adding a form of punishment for noncompliance. On the contrary, Colliver (2024) claimed that some tech companies were successful in dealing with specific areas regarding disinformation risk, especially in transparency for political advertising. However, COP's effectiveness was questioned in achieving the expected fundamental change due to its self-regulatory set-up and the lack of enforcement for non-compliance. "The Institute for Strategic Dialogue (ISD) calls for policymakers in the EU to design and enforce systemic transparency for advertising, content moderation, appeals, and redress systems, and algorithmic design and output to address the risks posed by disinformation in the European context" (Colliver, 2024).

Timm (2022) drew a discrepancy between Germany's and Sweden countermeasures against Russian misinformation. Sweden applies a mixture of different countermeasures of Confronting, Blocking, Naturalising, and Ignoring the Russian narratives. Confronting by disseminating its narrative to confront the foreign narrative, Blocking the opponent's narrative to control domestic exposure, Naturalising by promoting the self-image of the country and disregarding the other, and ignoring by not giving attention to the threat empowering citizens and institutions to criticize and contribute to the debate. In contrast, Germany tends to adopt the naturalizing approach and support national TV to confront the Russian narratives. Myers (2021) suggested that if citizens are more actively involved in the government's gathering and sharing of information, it can generate more public support and dismiss any arbitrary context drowned by conspiracy theories or foreign institutions. Such an approach can create stronger collaborative connections between the government, citizens, and local organizations to boost resilience and surveillance to detect any unexpected threats.

Soetekouw and Angelopoulos (2024) claimed that educating social media users by presenting related controversial topics, warnings and explanations can be more effective in enabling people to draw their informed conclusions. The inclusion of peer evaluation of the information's falsehood

AHMED SHEHATA: MISINFORMATION AND NATIONAL SECURITY: AN INTEGRATED FRAMEWORK FOR THREAT ANALYSIS AND INSTITUTIONAL RESILIENCE

(JSDS)

contributed to individuals' criticism of misinformation. Their implementation of protocol training for social media users revealed positive indicators of detecting fake news. They explained that age and level of education play a vital role in accepting fake news. There was a positive correlation between a higher level of detecting information and a higher level of education. While young users seemed to be more vulnerable to fake news than older people. Hence, educating people to enhance critical thinking in all walks of life can empower people to be more skeptical and more aware of filtering news credibility.

Law (2023) applied an experiential futures approach to predict and prototype to sample public feedback. Participants were exposed to physical items and audio-visual elements and were later asked to provide their responses, reactions, and perspectives. The fiction design reality simulation enabled participants to experience emerging futures and intervention scenarios allowing researchers to evaluate their responses and reactions to these futures. Results revealed that the participants most feared government and industry interventions, while community-based approaches were more favored. Cassar (2023) claimed that 90% of the participants consider that efforts to measure and curb misinformation's impact are insufficient. The public believes that the management of countering fake news relies on (29%) "News media publishers," "Non-governmental organizations (21.9%), "Government" (23.3%), "Big technological companies" (24%), and notable quantity pointed out that educational institution, regulatory authorities, and private sectors should be involved in curbing the dissemination of fake news.

 Humprecht et al. (2020) conducted empirical cross-national comparative research examining 18 Western democracies to understand the influence of politics, economy, and media environment on online disinformation. They claimed that political polarization could create a fertile ground for misinformation as it targets parting partisans, or elites on matters or policy spectrum (Dalton, 2008; Hetherington, 2001). They clustered the findings into three groups: 1- high resilience to disinformation (Northern and Western European countries like Austria, Belgium, Canada, Denmark, Finland, Germany, Ireland, the Netherlands, Norway, Sweden, Switzerland, and the U.K. including Canada), 2- low resilience (Southern European Countries as Spain, Italy, and Greece, and the US), 3- the US, as a unique case. The first group cluster stands out for welfare expenditure, support for mainstream broadcasting channels, well-structured regulation on media ownership, and advertising. Thus, they depicted a high level of mainstream media trust and low

fragmentation and polarization, which led to high resilience to disinformation. On the contrary, the second group was characterized by "late democratization, patterns of polarized conflict, a strong role of political parties, and dirigiste state interventions" (Humprecht et al., 2020). Consequently, trust in mainstream media is relatively low, while the consumption of information through social media is rather high. The third group was the US media as an exceptional phenomenon regarding online misinformation. The country stands out for its vast advertising market, weak mainstream media, and diverse politically polarized news streams. The competitive nature of its marketing culture has made the US attractive to disinformation-targeting social media users, resulting in low trust in mainstream media and a low resilience level to misinformation.

Fee 2021, examined resilience strategies employed by the United Kingdom (UK) and Sweden governments in combatting disinformation. The findings confirmed that both countries shared similar resilience strategies to reduce societal exposure to disinformation. Both countries sought to strengthen individual critical thinking and advocated media and information literacy through educational practices. They took part in distributing online checklists, governmental guidance, publications, and other strategies to overcome the misinformation wave. They both create independent journalism and media in and around misinformation actors, which in this case view Russia as a shared opponent and a creator of misinformation dissemination in both countries. They have issued policies to create, support, and promote independent journalism and media. Moreover,

Shaping the information environment to command the strategic narrative was viewed as effective by both countries. The policy approach through implementing fact-checking, targeted messaging, and communicative capacity in building and disseminating information was also favored in both countries.

Another study was carried out by Dragomir et al., 2024 to uncover the characteristic features of what makes countries vulnerable or resilient in encountering online disinformation in four countries (Austria, Czechia, Finland, and Spain). Austria is featured with a healthy level of democracy, government support for media, a diverse and vibrant media market (private and public), and complex media regulations depicting a high level of trust by its audience. Probably, the misinformation tsunami impact has implications for Austrian society. In response, the government implemented a combination of legislation, self-regulation, and literacy. Czechia is featured with solid democracy, strong public

AHMED SHEHATA: MISINFORMATION AND NATIONAL SECURITY: AN INTEGRATED FRAMEWORK FOR THREAT ANALYSIS AND INSTITUTIONAL RESILIENCE

(JSDS)

broadcasting channels, and low foreign ownership in private media. The media ecosystem in Czechia has been considered the healthiest in Europe. Nevertheless, the government displayed vulnerabilities to disinformation due to government weakness in detecting false narratives, weak involvement of community individuals, lack of media literacy, and a growing number of government-sponsored misinformation.

On the other hand, Finland is featured with strong democracy, strong institutionalized editorial freedom, free access to online content and services, and a healthy public media organization. Finland outstands other European countries as being accredited with top-ranking media literacy (Jaakkola, 2020), thus gaining public trust in government and national media streams. To respond to misinformation, the government implemented different approaches like fact-tracking, promoting educational activities, and encouraging free press attribution to innovate media literacy policies. However, some suggest legal legislation to control the velocity of misinformation. While Spain is featured with a strong democracy, it has poor freedom of the press, a poor subsidized electronic media system, less developed professionalization of journalism, and a highly polarized society due to partisan government, political parties, and business. In response to misinformation, Spain implemented a combination of legal and policy instruments, as well as some literacy initiatives, to suspense and mitigate offensive misinformation related to crime, hate, health, and threats to public order. The first conviction of spreading misinformation was a sentence of 15 months and a fine of €1620 (García, 2022).

With the implementation of such procedures, concerns about freedom of expression and speech have been debated widely in Spain. Finding a holistic and effective approach with government and community involvement would be more successful in mitigating misinformation.

Trecek-King & Cook (2024) piloted an Inoculation theory applying the biological concept of vaccination to misinformation and its effectiveness in building resilience in the science field.

7. METHODOLOGY

Description of the methodology followed in the study. This study employs a qualitative research design focused on systematic content analysis to develop an integrated framework for analyzing misinformation threats and institutional responses. The methodology centers on comprehensive analysis of existing literature, policy

documents, and institutional reports published between 2015 and 2024. This temporal boundary captures recent technological developments and emerging institutional responses while maintaining historical context.

Content analysis is the primary analytical approach, utilizing NVivo software for qualitatively coding the identified literature. The coding schema emerges from the iterative analysis of the texts, focusing on three primary dimensions: threat mechanisms, institutional responses, and resilience indicators. Two independent coders analyze the material to ensure analytical rigor, with inter-coder reliability assessed using Cohen's kappa coefficient. This process enables the systematic identification of patterns and themes while maintaining methodological transparency.

The framework development phase synthesizes insights from the content analysis through systematic comparison of findings across different national and institutional contexts. The analysis examines varying approaches to misinformation response and resilience building, particularly focusing on successful strategies and implementation challenges documented in the literature.

Data sources include major academic databases (Web of Science, Scopus, JSTOR), policy repositories, and institutional reports. The analytical procedure progresses from thematic analysis through comparative analysis to framework development, with each stage building upon insights from the previous phase. Quality assurance measures include rigorous documentation of analytical decisions, peer review of the coding schema, and comprehensive source verification.

This methodology enables systematic examination of misinformation threats while providing practical insights for institutional resilience building. The approach balances theoretical rigor with practical applicability, ensuring the resulting framework serves both academic and institutional needs.

8. RESULTS

Content analysis reveals the evolution of misinformation from state-sponsored propaganda to AI-enabled digital threats. The CIA's 1950s campaign against Guatemalan President Arbenz exemplifies early strategic misinformation (Law, 2023), while contemporary challenges show that 60.1% of users share content without verification (Cassar, 2023).

Misinformation manifests across multiple domains. During COVID-19, it generated widespread uncertainty and vaccine hesitancy through conspiracy theories. Financial markets face specialized websites combining credible and distorted

AHMED SHEHATA: MISINFORMATION AND NATIONAL SECURITY: AN INTEGRATED FRAMEWORK FOR THREAT ANALYSIS AND INSTITUTIONAL RESILIENCE

(JSDS)

content, impacting price actions and business operations (Belova & Georgieva, 2018).

Cross-national analysis reveals varying institutional responses and vulnerabilities (see figure 1). Countries with high polarization and little press freedom show heightened concerns about misinformation. Nations with an independent press and low polarization demonstrate greater resilience (Van et al., 2024). The European Commission's Code of Practice on Disinformation, launched in 2018 and revised in 2021, represents a significant initiative but challenges implementation (Pamment, 2022).
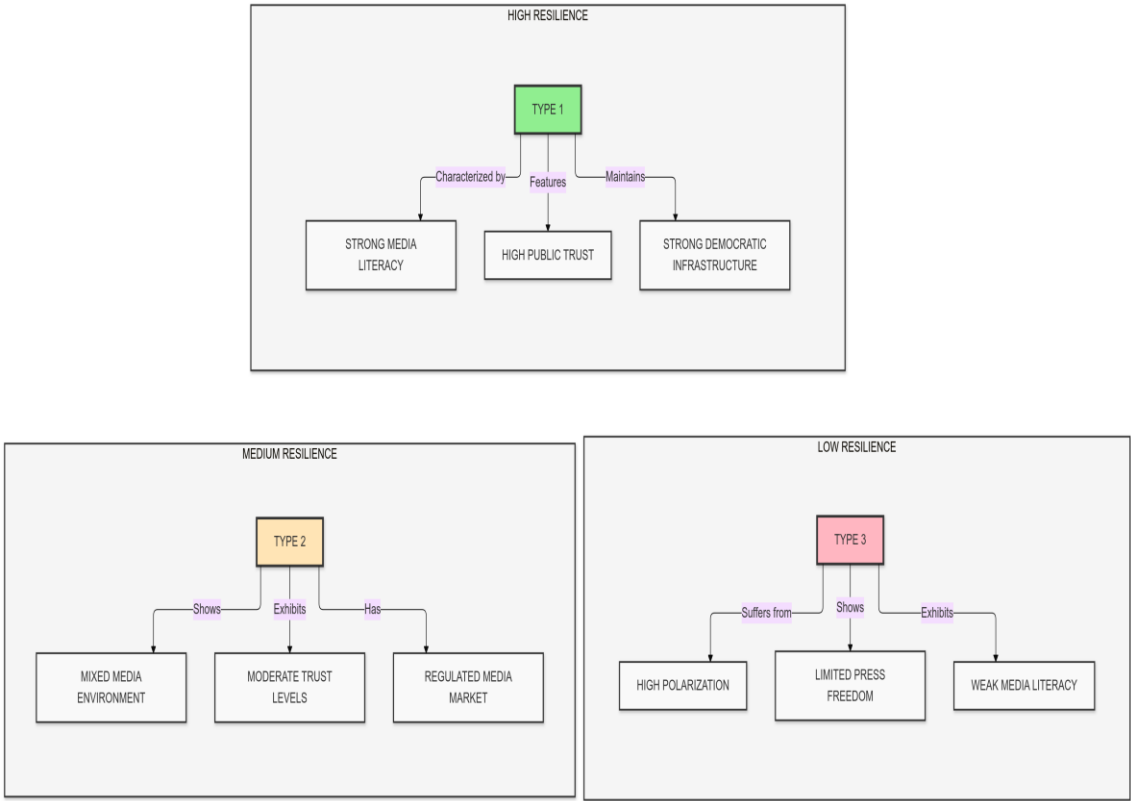

FIGURE 1. Cross-national variation in institutional resilience

Analysis of the literature identifies four critical dimensions for institutional resilience against misinformation:

- Structural Resilience emerges through media market diversity, regulatory frameworks, and democratic infrastructure. Evidence from Finland and Austria demonstrates how strong democratic institutions and regulated media environments enhance resilience. Finland's top-ranking media literacy and strong public trust contrast with Spain's challenges from poor press freedom and societal polarization (Dragomir et al., 2024).
- Educational Capacity manifests in media literacy programs and professional development. Research shows a direct correlation between education levels and misinformation detection abilities, with age playing a significant role. Young users show greater vulnerability to fake news compared to older demographics (Soetekouw & Angelopoulos, 2024).
- Response Mechanisms require coordinated stakeholder action. Sweden demonstrates success through multiple strategies: confronting, blocking, naturalizing, and ignoring misinformation narratives. Germany focuses primarily on naturalizing approaches and supporting national television (Timm, 2022).
- Societal Trust fundamentally shapes resilience. Studies show responsibility distribution among stakeholders: news media publishers (29%), non-governmental organizations (21.9%), government (23.3%), and technology companies (24%) (Cassar, 2023).

Based on these findings, we propose the Institutional Resilience Framework Against Misinformation (IRFM), which systematically addresses identified challenges and integrates successful approaches from multiple national contexts (Figure 2).
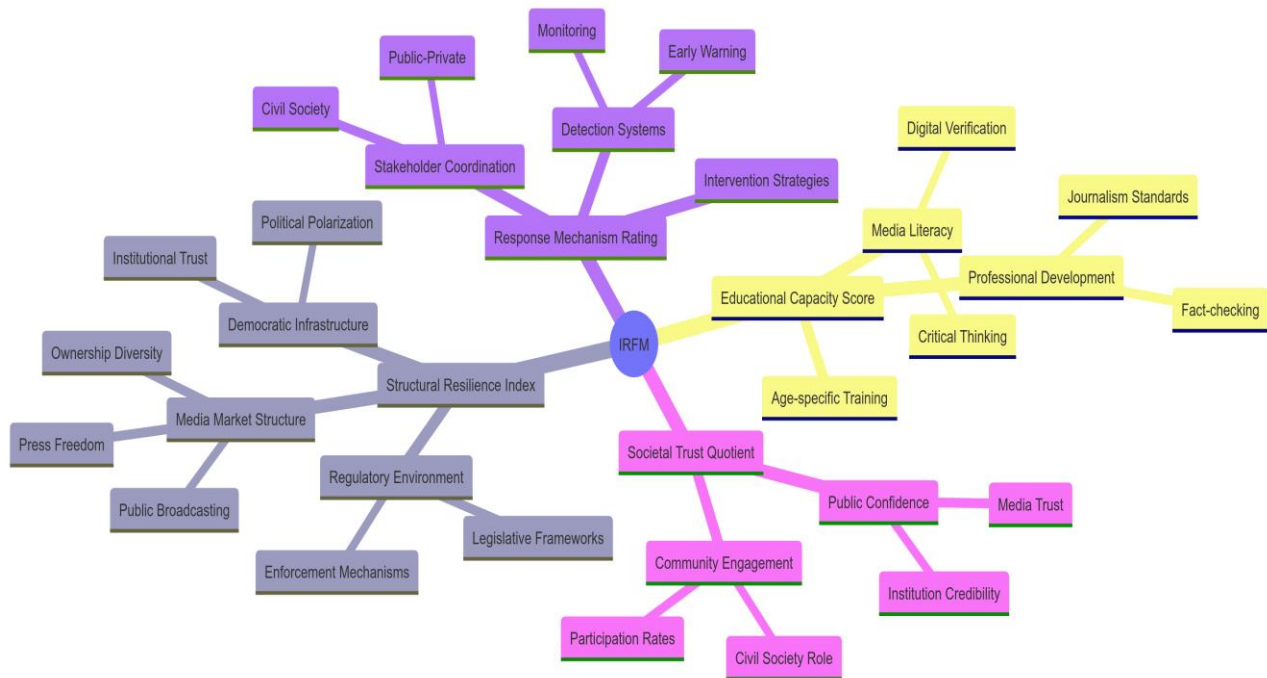
AHMED SHEHATA: MISINFORMATION AND NATIONAL SECURITY: AN INTEGRATED FRAMEWORK FOR THREAT ANALYSIS AND INSTITUTIONAL RESILIENCE

(JSDS)

FIGURE 2. The proposed IRFM structure and components.

The IRFM comprises four integrated components:

1. Structural Resilience Index (SRI)

SRI measures three key elements:

- Media Market Structure: Assesses media ownership diversity and market concentration ratios based on evidence from Austria's diverse media market (Dragomir et al., 2024). Includes metrics for public broadcasting strength and independence.
- Regulatory Environment: Evaluates legislative frameworks and enforcement mechanisms, incorporating lessons from the EU's Code of Practice on Disinformation (Pamment, 2022).
- Democratic Infrastructure: Measures political polarization levels and institutional trust, reflecting findings on polarization's role in misinformation vulnerability (Humprecht et al., 2020).

2. Educational Capacity Score (ECS)

ECS evaluates:

- Media Literacy Programs: Measures critical thinking development and digital verification skills, based on Finland's successful model (Dragomir et al., 2024).
- Professional Development: Assesses journalism standards and fact-checking protocols.
- Age-specific Training: Addresses varying vulnerability across age groups (Soetekouw & Angelopoulos, 2024).

3. Response Mechanism Rating (RMR)

RMR examines:
- Detection Systems: Evaluates early warning indicators and monitoring protocols, drawing from Sweden's comprehensive approach (Timm, 2022).
- Stakeholder Coordination: Measures public-private partnerships and civil society engagement effectiveness.
- Intervention Strategies: Assesses content moderation policies and counter-narrative capabilities.

4. Societal Trust Quotient (STQ)

STQ measures:
- Public Confidence: Evaluates institutional credibility and media trust.
- Community Engagement: Assesses public participation and civil society involvement.
- Transparency Measures: Evaluates institutional communication effectiveness.

The framework implementation follows four phases:

Phase 1 - Assessment: Institutional evaluation using the four components

Phase 2 - Strategy Development: Priority identification based on assessment results

Phase 3 - Implementation: Coordinated deployment of identified strategies

Phase 4 - Evaluation: Impact measurement and strategy refinement.

Each component's metrics are weighted based on empirical evidence from successful national models, particularly drawing from high-resilience countries identified in the

AHMED SHEHATA: MISINFORMATION AND NATIONAL SECURITY: AN INTEGRATED FRAMEWORK FOR THREAT ANALYSIS AND INSTITUTIONAL RESILIENCE

(JSDS)

literature. The framework provides both diagnostic tools for assessing institutional vulnerability and strategic guidance for building resilience against misinformation threats.

9. DISCUSSION

The IRFM synthesizes empirical evidence into an actionable framework for building institutional resilience against misinformation. Each component addresses specific vulnerabilities identified in the literature while incorporating successful practices from high-resilience nations.

The SRI's emphasis on media market structure reflects findings from Austria and Finland, where diverse media ownership and strong public broadcasting correlate with higher resilience (Dragomir et al., 2024). The inclusion of democratic infrastructure metrics acknowledges the critical role of political polarization in institutional vulnerability, particularly evident in Spain's experience with partisan pressures.

The ECS component builds on Finland's successful media literacy model while addressing age-related vulnerabilities identified by Soetekouw and Angelopoulos (2024). The framework's professional development metrics respond to evidence linking journalism standards to institutional resilience, addressing gaps identified in countries with less developed media professionalization.

The RMR's multi-stakeholder approach incorporates lessons from Sweden's comprehensive strategy (Timm, 2022), while addressing coordination challenges identified in the EU's Code of Practice implementation (Pamment, 2022). The framework's emphasis on detection systems responds to the evolving nature of AI-enabled misinformation threats identified by Cassar (2023).

The STQ component addresses the fundamental role of public trust, reflecting findings from cross-national studies showing correlation between institutional trust and misinformation resilience (Humprecht et al., 2020). The framework's attention to community engagement responds to evidence that public participation strengthens institutional defense against misinformation.

However, implementation challenges remain. The framework's effectiveness may vary in highly polarized environments with compromised institutional trust. Additionally, rapid technological evolution may require continuous adaptation of assessment metrics. Future research should focus on validating the framework's effectiveness across different political and social contexts.

10. CONCLUSION

This study has developed the Institutional Resilience Framework Against Misinformation (IRFM) through systematic analysis of institutional responses to misinformation threats. The framework integrates structural, educational, response mechanism, and societal trust components, providing measurable metrics for assessing and building institutional resilience.

Analysis reveals significant variation in institutional responses across nations, with Northern European countries demonstrating higher resilience through regulated media environments and strong democratic institutions. The framework addresses identified gaps in current approaches, particularly in coordinating multi-stakeholder responses and building public trust.

The IRFM's primary contribution is its systematic approach to measuring and strengthening institutional resilience, incorporating successful practices from high-resilience nations while maintaining adaptability to local contexts. Future research should focus on framework validation across different political and social environments, particularly in highly polarized contexts where institutional trust faces significant challenges.

REFERENCES

Adeyemi, O. A., & Kisugu, O. A. M. (2022). Fake news its implication for national security in Nigeria. International Journal of Academic Multidisciplinary Research, 6(11), 54-59.

Amazeen, M. A. (2024). The misinformation recognition and response model: An emerging theoretical framework for investigating antecedents to and consequences of misinformation recognition. Human Communication Research, 50(2), 218-229.

Belova, G., & Georgieva, G. (2018). Fake news as a threat to national security. In International Conference Knowledge-Based Organization (Vol. 24, No. 1, pp. 19-22).

Calvillo, D. P., Garcia, R. J., Bertrand, K., & Mayers, T. A. (2021). Personality factors and self-reported political news consumption predict susceptibility to political fake news. Personality and Individual Differences, 174, Article 110666.

Cassar, D. (2023). The misinformation threat: A techno-governance approach for curbing the fake news of tomorrow. Digital Government: Research and Practice, 4(4), Article 3631615. https://doi.org/10.1145/3631615

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202-215.

Colliver, C. (2024). Cracking the code: An evaluation of the EU code of practice on disinformation. Institute for Strategic Dialogue.

Daunt, K. L., Greer, D. A., Jin, H. S., & Orpen, I. (2023). Who believes political fake news? The role of conspiracy mentality, patriotism, perceived threat to freedom, media literacy and concern for disinformation. Internet Research, 33(5), 1849-1870.

Dragomir, M., Rúas-Araújo, J., & Horowitz, M. (2024). Beyond online disinformation: Assessing national information resilience in four European countries. Humanities and Social Sciences Communications, 11(1), 1-10.

Dumitrache, V., & Popa, B. (2022). How the fake news and disinformation impact national security: Case study from the COVID-19 pandemic. Military Science Universe Journal.

AHMED SHEHATA: MISINFORMATION AND NATIONAL SECURITY: AN INTEGRATED FRAMEWORK FOR THREAT ANALYSIS AND INSTITUTIONAL RESILIENCE

(JSDS)

Englmeier, K. (2021). The role of text mining in mitigating the threats from fake news and misinformation in times of corona. Procedia Computer Science, 181, 149-156.

European Commission. (2022, June 16). The strengthened code of practice on disinformation. https://test2.disinfocode.eu/wp-content/uploads/2023/01/The-Strengthened-Code-of-Practice-on-Disinformation-2022.pdf

Harcup, T., & O'Neill, D. (2017). What is news? News values revisited (again). Journalism Studies, 18(12), 1470-1488.

Humprecht, E., Esser, F., & Van Aelst, P. (2020). Resilience to online disinformation: A framework for cross-national comparative research. The International Journal of Press/Politics, 25(3), 493-516.

Law, J. (2023). Building mental resilience against disinformation: An experiential futures case study. Journal of Future Studies.

Lee, T. (2019). The global rise of "fake news" and the threat to democratic elections in the USA. Public Administration and Policy, 22(1), 15-24.

Lo Sardo, D., Brugnoli, E., Gravino, P., & Loreto, V. (2024). From Trust to Disagreement: disentangling the interplay of Misinformation and Polarisation in the News Ecosystem.

Monteith, S., Glenn, T., Geddes, J., Whybrow, P., Achtyes, E., & Bauer, M. (2023). Artificial intelligence and increasing misinformation. The British Journal of Psychiatry, 224, 33 - 35. https://doi.org/10.1192/bjp.2023.136.

Myers, N. (2021). Information sharing and community resilience: Toward a whole community approach to surveillance and combatting the "infodemic". World Medical & Health Policy, 13(3), 581-592.

Newman, N., Fletcher, R., Eddy, K., Robertson, C. T., & Nielsen, R. K. (2023). Reuters Institute digital news report 2023. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023

Nyhan, B., & Reifler, J. (2019). The roles of information deficits and identity threat in the prevalence of misperceptions. Journal of Elections, Public Opinion and Parties, 29(2), 222-244.

Ognyanova, K., Lazer, D., Robertson, R. E., & Wilson, C. (2020). Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. Harvard Kennedy School Misinformation Review.

Fee, J. P. (2021). Resilience against the dark arts: A comparative study of British and Swedish government strategies combatting disinformation [Unpublished manuscript].

Firdaus, N., Jumroni, J., Aziz, A., Sumartono, E., & Purwanti, A. (2024). The influence of social media, misinformation, and digital communication strategies on public perception and trust. The Journal of Academic Science, 1(3), 131-138.

Pamment, J. (2020). The EU code of practice on disinformation: Briefing note for the new EU commission. Carnegie Endowment for International Peace.

Soetekouw, L., & Angelopoulos, S. (2024). Digital resilience through training protocols: Learning to identify fake news on social media. Information Systems Frontiers, 26(2), 459-475.

Sultan, K., & Zaman, A. (2023). A Study on Evaluating the Impact of Social Media's Fake News on The Attitudes and Beliefs of a Society. International Journal of Social Science & Entrepreneurship. https://doi.org/10.58661/ijsse.v3i4.228.

Timm, C. (2022). Strategies and resilience against disinformation influences [Master's thesis]. Lund University. https://lup.lub.lu.se/student-papers/search/publication/9070305

Trecek-King, M., & Cook, J. (2024). Combining different inoculation types to increase student engagement and build resilience against science misinformation. Journal of College Science Teaching, 53(1), 1-6.

Van der Meer, T. G., & Hameleers, M. (2024). Misinformation perceived as a bigger informational threat than negativity: A cross-country survey on challenges of the news environment. Harvard Kennedy School Misinformation Review.

Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe.

Jaakkola, M. (2020). Editor's introduction. Media and information literacy research in countries around the Baltic Sea. Central European journal of communication, 13, 146-161. https://doi.org/10.19195/1899-5101.13.2(26).1.

Serrano-Puche, J., Rodríguez-Salcedo, N., & Martínez-Costa, M. (2023). Trust, disinformation, and digital media: Perceptions and expectations about news in a polarized environment. El Profesional de la información. https://doi.org/10.3145/epi.2023.sep.1