

REVIEW

Open Access



A multivocal grey literature review on fake news and risk management

Eduardo Noronha^{1,2*}, João Varela da Costa^{1,2} and Miguel Mira da Silva^{1,2}

*Correspondence:

Eduardo Noronha
eduardo.noronha@inov.pt
¹INESC INOV, Lisbon Portugal, Rua
Alves Redol, 9, Lisboa
1000-029, Portugal
²Universidade de Lisboa, Instituto
Superior Técnico, Campus da
Alameda, Avenida Rovisco Pais,
Lisboa 1049-001, Portugal

Abstract

The proliferation of fake news presents an emerging and complex cybersecurity challenge in the realm of information systems, with significant implications for security. This study investigates the intersection of fake news and risk management through a Multivocal Literature Review, drawing from academic research, professional practice, and grey literature. The findings demonstrate how fake news acts as a cyber-enabled threat, amplifying risks and complicating decision-making and risk mitigation. Considering the interdisciplinary nature of cybersecurity and modern management, addressing fake news requires integrated strategies that combine technological innovation, policy development, and education. This research emphasizes the importance of proactive prevention, mitigation, and strategic recovery to enhance resilience against information manipulation. By synthesizing diverse perspectives, the study contributes to the broader discourse on data, information, and management security, and advocates for collaborative solutions to strengthen digital trust and organizational integrity. It also identifies key directions for future research, underscoring the need for continuous adaptation in managing the evolving landscape of cyber-enabled disinformation.

Keywords Fake news, Risk management, Digital risk, MLR

1 Introduction

The era of digitalization, where technologies appear and evolve at an unprecedented pace, has transformed how we access, share, and utilize information, bringing numerous benefits such as faster communication and innovative solutions to complex challenges. However, alongside the advancements, it has also brought and developed new risks that need to be considered [30]. Due to these modern risks, a branch of risk defined as digital risk has appeared and has grown together with technology, presenting new challenges and threats to risk management.

Risk management is the systematic process of identifying, analyzing, evaluating, treating, monitoring and communicating risks to ensure the achievement of goals across an organization International Organization for Standardization [22]. It plays a crucial role across various domains, from finance to public safety, providing structured approaches to handle uncertainties.



© The Author(s) 2026. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

The theme of this paper, fake news, is one of the threats of risk management that has been growing recently. Although it is a problem that has been present throughout the history of humanity, with the modern world of digitalization, fake news has emerged as a widespread and damaging phenomenon. Presented now as a cyber risk [31], it poses risks to public safety, democratic processes, and social cohesion. The rapid proliferation of social networks and online communication channels has amplified the reach and influence of fake news, enabling it to spread at unprecedented speeds and with greater ease for perpetrators. The connection between people from around the world and the ease of sharing information swifts the propagation of information away from professional journalism, facilitating the spread of fake news [25]; this undermines trust in individuals and institutions, and results in consequences that can range from inexistant to threatening for regimes and democracy. Innovative solutions are required to tackle this issue and mitigate its effects on communities, as the specific nature of fake news and its rapid evolution make traditional risk management approaches inadequate [48].

Despite the increasing recognition of fake news as a form of digital risk, existing literature remains fragmented in its treatment of the topic within the context of risk management. Many studies have examined fake news from perspectives such as communication, psychology, and computer science, focusing primarily on its detection, dissemination patterns, or social implications. However, fewer studies have systematically explored fake news as a risk phenomenon. As a result, there is a critical research gap in mapping fake news within established risk taxonomies. Addressing this gap is essential to developing a more comprehensive understanding of digital risks and strengthening the resilience of modern information ecosystems.

This study proposes conducting a multivocal literature review (MLR) to enhance our understanding of the complexities of fake news and its characterization as a threat within the risk management domain. The review will explore existing research on the topic, focusing on defining fake news, its key concepts, and their connection with risk management.

The report adopts a structured approach, beginning with the chosen research methodology. A background on risk management and fake news follows this. Subsequently, the MLR is presented, which includes the planning phase of the MLR, the motivation for the review, the research questions defined, the data collection, the responses to the research questions, and finally, a discussion of the results.

2 Research background

This section aims to address two fundamental topics related to this research, Risk management and Fake news, setting the groundwork for the continuity of this study.

2.1 Risk management

Risk is the effect of uncertainty on objectives [35]. It can disrupt activities, damage goods and reputations, and create havoc, both in organizational and in society. Therefore, managing risk is essential.

Risk management is the process of identifying, classifying, analyzing, and assessing risks to avert potential problems [13]. In recent years, with the introduction of digital risk and an ever more existing global reach, which in turn leads to long-lasting consequences in terms of reputation, increasing efforts have been made in implementing

proactive risk management measures, as with these, organizations can mitigate losses, bolster resilience, and facilitate informed decision-making, thereby improving overall performance. Numerous prevalent frameworks currently provide risk management guidelines, with special regard to ISO 31,000 (International Organization for Standardization [22], an international standard focusing on generating value for organizations by recognizing and reducing risks that may affect critical objectives [13] also outlines the procedures involved in risk management, dividing them into these phases:

- Plan: This stage involves establishing the importance of risk management, allocating resources and time, and laying the groundwork for risk evaluation.
- Identification: Includes identifying the many kinds and origins of risks, recognizing possible risk situations, and defining who is responsible for dealing with them.
- Analysis: Assessing the priority of identified risks.
- Response: Developing strategies based on the risks involved in minimizing threats to objectives.
- Monitor and Control: identifying the expected risks and tracking them, implementing risk response plans, monitoring residual risks, and evaluating the effectiveness of risk management.

New issues and trends are progressively influencing modern risk management. Complex cybersecurity threats such as fake news have been brought about by the growth of digital technology, creating the need for enterprises and organizations to use sophisticated risk assessment techniques and tools. Thus, risk management should be dynamic and iterative, allowing for continuous improvement in response to evolving risks and conditions [9].

2.2 Fake news

Fake news, a term that has gained significant traction in recent years, poses a complex problem in modern culture, particularly within the digital media ecology [6]. Even though the term “fake news” has been prevalent in recent years, the phenomenon itself is not new [18]. Propaganda and misinformation have long been used to sway public opinion. This practice dates back to ancient times when political leaders disseminated misinformation to stay in power.

Throughout the years, fake news has been intertwined with technological advancements. The propagation of false information through well-known media outlets like CNN and The New York Times during the Iraq War and William Randolph Hearst’s war-mongering journalism preceding the Spanish-American War in 1897 demonstrate how information has been manipulated for political ends throughout history [18]. However, the era of information and the rise of social media has brought fake news to a different scale. The spread of fake news has accelerated massively [1], which, together with the decentralized nature of the internet and an algorithmic manipulation that prioritizes engagement over veracity, makes it more challenging to discern between genuine and untrustworthy sources of information.

In recent years, there have been several situations where fake News took an important part in real-world events, with one of the most prominent examples being the Brexit referendum, where fake news, such as the claim that the UK sent £350 million per week to the European Union, became a focal point of debate and, even though the claim was

later denied, it fueled resentment toward the European Union [27]. It reinforced the idea that leaving the union would free up substantial funds for other domestic programs. The appearance of sophisticated disinformation tools, such as deepfakes, has only made it worse for the efforts against fake news [8] and has increased the need for greater control against disinformation.

Fake news can be defined differently by distinct authors [1] acknowledge the lack of a universally accepted definition of fake news, stressing that fake news closely resembles the truth, making it challenging for AI-based platforms to distinguish fake news without external human validation. Their review highlights the intricate interactions between intent, authenticity, and knowledge by classifying definitions of fake news. Other studies, such as [28], highlight that some factors that are closely aligned with fake news are not sufficient to define them, such as:

- **Truth Value:** To be considered fake news, information must be more than false. Even if a made-up story turns out to be real, it might still be deemed false news because the person who created it had no way of knowing it was true.
- **Source:** Although fake news frequently comes from unreliable sources, respectable media organizations may unintentionally contribute to its spread. On the other hand, information from a less reliable source may be factual and thoroughly investigated.
- **Presentation:** Techniques such as clickbait and other tactics used to increase user engagement, although typical features of modern fake news, are not unique to fake news. Sensationalist presenting techniques can also be used by legitimate news organizations under economic pressure; therefore, the presentation is insufficient to classify an article as fake news.

Various initiatives have been proposed and developed to help users identify credible sources and verify information in response to the rise of fake news, with solutions ranging from human led efforts to sophisticated algorithmic systems [16].

Social media corporations such as Facebook and Twitter have already implemented fact-checking methods [40], which flag postings with unconfirmed claims and reduce their visibility. Giving people the ability to assess information critically is essential for spotting and halting the spread of fake news, and ideas such as using artificial intelligence to analyze content and identify fake news patterns are becoming more realistic than ever. Models and techniques rooted primarily on machine learning and deep learning are being rapidly developed, especially in the context of social media where fake news spreads exponentially [2]. However, AI-based solutions may still require factual confirmation from humans [1]. Alemanno [3] proposes strategies to counter the fake news problem, highlighting an approach that should address the issue on individual, societal, and technological levels. This approach focuses on four steps: empowering individuals by having media literacy as a first line of defense; utilizing technological solutions such as artificial intelligence and collaborative fact-checking platforms for detection and verification; systemic approaches through the promotion of responsible social media practices and addressing social media algorithm bias; and finally, cultivating a culture of critical thinking, by motivating individuals to seek multiple perspectives on the same subject.

In summary, fake news is not a new obstacle, but the digital era has made it harder to tackle, and innovative measures can and should be made to mitigate its impact on society.

3 Research questions

This study uses an exploratory approach to comprehensively understand fake news and its relationship to digital risk management. Because of fake news' intricacy and multi-disciplinary character, the investigation concentrates on both the theoretical and practical facets of the subject. This comprehensive investigation aims to identify fundamental ideas, develop connections between them, and examine how they relate to digital risk management's broader domain.

Four research questions (RQs) have been formulated to guide this investigation. These aim to define fake news, identify its main concepts, explore the interconnections between these concepts, and examine how they relate to digital risk management:

- RQ 1 – How is Fake News defined?
- RQ 2 – What are the main concepts in Fake News?
- RQ 3 – What is the inter-relationship between the identified concepts of Fake News?
- RQ 4 – What is the relationship between the concepts of Fake News and Digital Risk Management?

4 Research methodology

This study employs an MLR methodology, which expands the conventional systematic literature review (SLR), by including both grey literature (GL) and peer-reviewed scholarly sources, to thoroughly examine the existing information on fake news and risk management. As an SLR on the subject already exists, it presented an opportunity to use this method, as it allows not only for bridging the gaps between theory and practice and for including different views on the matter but also to compare the results of the MLR with those of the SLR.

The primary challenges of MLRs relate to the variability, control, and quality of grey literature sources compared to formally published academic papers. MLRs find their value in providing multiple perspectives on the subject but also picks new problems earlier than with thorough academic research, which has extreme importance in an upcoming topic such as fake news and its connection with risk management [17] defines guidelines on incorporating GL in an MLR. The process is divided into three parts:

1. Planning: Where the motivation for conducting an MLR is explained and the research questions are defined,
2. Conducting: This includes the search process, the collection of data, and its analysis,
3. Reporting: Where the research questions are answered in detail with resources to the data previously extracted.

To conduct the process, both these guidelines and the work from [26] were considered. Figure 1, presented below, summarizes the three phases and their key steps.

4.1 Planning phase

The initial stage of the MLR involves outlining the implementation of the review process and establishing its key elements. This phase begins with the motivation for the review,

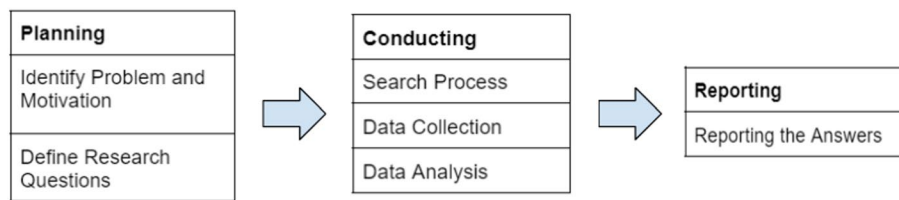


Fig. 1 MLR phases as per [26]

followed by the formulation of research questions and the development of search criteria and protocol.

4.1.1 Motivation

Due to society's rapid digitalization and the growth of social media, the way information is created, shared, and consumed has changed significantly [1]. Among these developments, the spread of fake news has become a significant concern for people, institutions, and governments. In the larger framework of digital risk management, it is critical to address the pervasiveness of inaccurate or misleading information, namely fake news, since it poses serious risks to decision-making, public trust, and business reputation.

Comprehending the phenomenon of fake news is crucial for both scholarly investigations and real-world uses, as having depth insights into the subject catalyzes the development of solutions for the problem [44]. However, the phrase itself is frequently employed inconsistently across different sectors due to its complex nature, which encompasses inaccuracy, disinformation, credibility, and intent. As a result, our knowledge of its extent and effects is fragmented. A thorough examination of the fundamental ideas and connections that characterize fake news in a digital setting is, therefore, urgently needed.

Furthermore, little attention has been paid to the relationships between fake news and digital risk management. Businesses are becoming more aware of the dangers of fake news, including the possibility of money losses, reputational harm, and cybersecurity flaws. Despite these dangers, a precise framework that connects fake news to more general digital risk domains has not yet been completely developed. This study aims to create a coherent understanding of fake news and its significance for controlling digital risks by analyzing existing literature and combining knowledge from other fields. The motivation behind this review can be divided into four different goals:

- Clarify the definition of fake news and its concepts: Research on fake news and creating workable solutions to lessen its impact depend on a comprehensive, coherent understanding of the term. This examination will offer an organized basis for comprehending how fake news operates and propagates in the digital world by recognizing and categorizing the fundamental ideas associated with fake news.
- Linking fake news to digital risk management: Although fake news has historically been researched in disciplines like political science and media studies, little is known about how it affects business risk management tactics. By examining the connection between fake news and digital risk management, this analysis seeks to close this gap by highlighting the distinct and changing risks that fake news presents in the digital era.
- Demonstrate the benefits of complimenting a systematic literature review with grey literature: fake news dynamic and rapidly evolving nature, especially in digital

contexts, necessitates an approach beyond academic sources alone. Grey literature often provides timely and practical perspectives absent from peer-reviewed academic studies. By incorporating grey literature alongside a systematic literature review, this research will ensure a more comprehensive analysis, offering a balanced view that combines rigor with contemporary relevance.

4.2 Conducting

This section describes the search process for the necessary information for a MLR.

4.2.1 Search process

As a systematic literature review already exists, the goal of this study is to compile a MLR, which also adds grey material to support the systematic literature review. “Grey literature” describes sources that help comprehend the research topic but are not released through conventional academic channels. These may include:

- Technical reports from government agencies, industry, or academic institutions.
- White papers published by businesses and trade associations.
- Conference proceedings and presentations.
- Blog entries, discussion forums, and expert commentaries.
- Policy briefs and working papers.

The search consisted of the use of the search string (“Fake news” and “risk management”) in Google search in order to include all results that manifested both expressions so that the relation between the two terms was present, to make sure it was possible to address the scope of the review on the intersection of fake news and risk management. Figures describing the results can be seen in Sect. 5.5, while the results of the extraction are available in the tables 4 and 5 in the [Appendix](#).

Both academic and grey literature were accepted or rejected based on the inclusion and exclusion criteria in the following subsection.

4.2.2 Inclusion and exclusion criteria

Several criteria were applied based on the research to determine which articles and publications would be included in the review, considering the distinct nature and research methods of grey-and-white literature from [17]. A set of criteria for inclusion and exclusion (IC and EC, respectively) was applied:

- IC1: The concepts of both fake news and risk management were present.
- IC2: Relevance to the Research Questions.
- EC1: Results were not written in the English or Portuguese language.
- EC2: Inability to access source content.
- EC3: Out of Scope content.
- EC4: Advertisements for products or services.

Results were not rejected based on the type of article or publication retrieved, as blogs, newspaper articles, reports, academic papers, dissertations, and others were all considered important results for this review. Since the search engine used for the research was Google, which has no clear end to the number of results found, it was decided that data collection would end upon the exclusion of ten consecutive results.

4.2.3 Initial analysis/abstract reading

In the initial analysis of the results, the abstract of every paper found was read to verify whether it would be included or excluded in the research analysis. Other types of information, such as blogs, articles, presentations, introductions, and conclusions, were read in full, (in cases where the literature was extensive, only the introduction and conclusion were read at this stage), to verify whether the content was also interesting for the research. “Excluded” results were immediately eliminated, while “included” results would move on to the next review phase.

4.2.4 In-depth analysis/full reading

After the initial screening, the selected grey literature will undergo a full, in-depth analysis. This step aims to thoroughly understand each document’s contributions. In this process, each document was read in full, with detailed notes taken on the key findings that could aid in responding to the research questions defined. If, during the analysis, it was found that the piece was not relevant to the research, it was discarded. If the analysis was completed, the paper was included in the final list. After this step, twenty-three results were found.

4.2.5 Extraction

With the search string (“Fake news” and “risk management”), which took into consideration “IC1”, thousands of results were found. Höchstötter [21] work concluded that the first 20 results in a search engine contain the majority of relevant results, with rapid decline afterwards. This led to the decision of stopping the search, after 10 straight results were discarded in the abstract reading stage, which led to only the first 112 results being studied. After the “initial analysis/abstract reading” phase and considering both the inclusion and exclusion factors, 28 results remained. After the “in-depth analysis/full reading” phase, 23 results were deemed final for the reporting.

Figure 2 shows the data collection process, represented in BPMN, while Fig. 3 shows the division of the selected articles by publication year.

The evolution of academic publications on fake news reflects major global events that heightened public concern about fake news. The first significant spike occurred in 2017 and 2018, which can be explained by events such as the United States presidential elections [4] and the Brexit referendum [27], which revealed the political influence of online disinformation. After a period of steady growth, a new and sharper rise appeared after

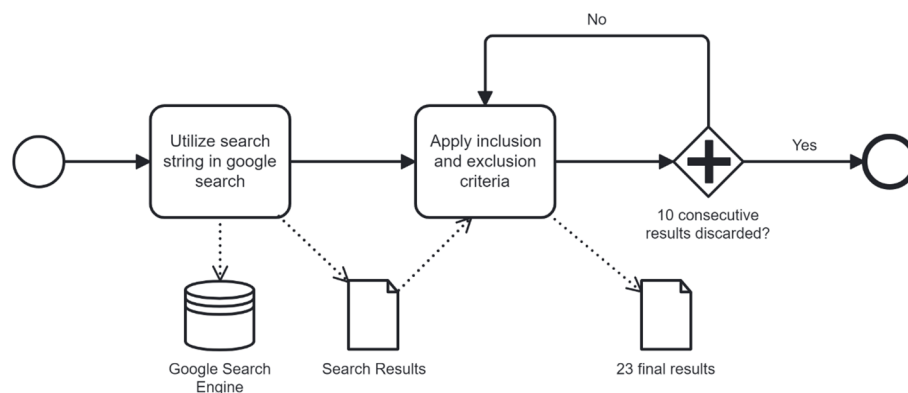


Fig. 2 Data collection process in BPMN. (Source: Author's on creation)

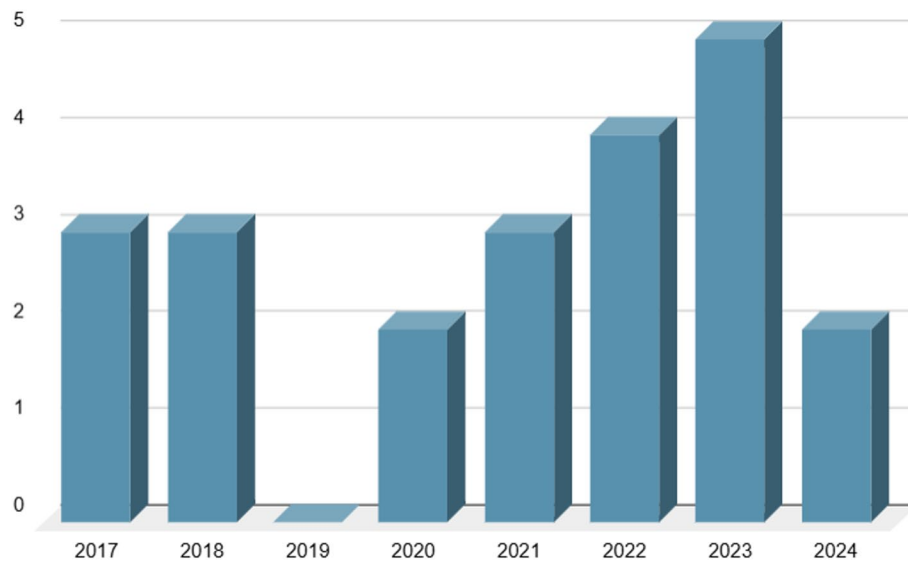


Fig. 3 Accepted results per year. (Source: Author's on creation)

2020, coinciding with the COVID-19 pandemic. During this time, the spread of health-related fake news became a serious public health threat, as demonstrated by [37]. This pattern indicates that moments of global crisis, whether political or health-related, directly amplify both the impact and the academic attention devoted to the study of fake news.

5 Reporting

The following section addresses the research questions established in the earlier stages of this study, with each subsection corresponding to a specific research question, providing a structured and comprehensive analysis based on the synthesized literature.

RQ 1 – How is Fake News defined?

Fake news is a topic that has always existed but has dramatically grown in importance in the last few years due to the rise of the information age. It is harmful, not only to individuals or society but also to brands and, therefore, can create all sorts of victims.

Fake news may be differently defined depending on the authors of the definition, with these definitions including fabricated news, false information that is spread, or even accurate information that is taken out of context to be disseminated. To better understand the definition of the term, it is of the utmost importance to understand the several different words and terms used to describe fake news. Table 1 contains the terms for fake news found in the articles, their definitions, and the number of papers they were found in.

The table demonstrates that fake news may be used and interpreted differently [12]. Define it as “false or misleading information that is spread rapidly either intentionally or unintentionally”. They characterize it by its potential to widely impact society due to the possibility of massive dissemination of false information. Alternatively, [32] describes fake news as “news that conveys or incorporates false, fabricated, or deliberately misleading information, ” being associated with social media and media platforms that can create havoc on society and elections through false information. Multiple studies, blogs,

Table 1 Definitions of fake news

Term	Definition	Papers
Misinformation	Misinformation refers to false information that is spread without malicious intent.	16
Disinformation	Disinformation refers to false information or information without context, that is spread intentionally with malicious intent.	10
False Information	False information refers to information that is not true. This is information that may be spread intentionally or unintentionally and can diverge from having great impact to no impact at all.	10
Misleading Information	Misleading information refers to both misinformation and disinformation, which means that it can be spread intentionally and unintentionally and may lead people to store and understand information and news that are not true.	9
Fabricated Information	Fabricated information is false information that is created with the intent of being spread. The information may be spread as true or false but is always created with the knowledge of being fake.	4
Propaganda	It refers to campaigns of dissemination of information, with the motivation of promoting an agenda, which may diverge from political, criminal, or simply for monetary gain.	4
Information Distortion	Information distortion is defined as risks that affect the flow of information, which may lead to disruption if happening within a supply chain.	1
Mal-information	Mal-information is defined as “accurate information taken out of context with the intent to harm”.	1

and articles can define fake news in slightly different forms, and understanding these various definitions and insights is crucial to better tackling the problem of fake news.

RQ 2 - What are the main concepts of Fake News?

The main concepts of fake news can take different forms and definitions throughout distinct research, but they are important to apprehend in order to understand their relation. Table 2 shows these concepts.

This table contains various concepts related to fake news and their definitions. These are the concepts that best relate to fake news, and it is of the utmost importance to understand each of these concepts and their role in the problem of fake news. With the ever-growing ease of spreading and sharing information, fake news's impact is increasing every year, affecting society through individuals, communities and brands. To mitigate this impact, it is essential to monitor social media activity in order to analyse the information shared publicly and to ascertain its content's validity and reliability, verifying as well if the context in which the information is made available is correct. In a digital landscape shaped by deepfakes that distort reality, echo chambers that reinforce existing beliefs, and truthiness that prioritizes emotional conviction over factual accuracy, understanding these dynamics is crucial to combating the spread of fake news. These efforts reduce the dissemination of misleading information and, therefore, contribute to the demise of fake news' impact.

RQ 3 – What is the inter-relationship between the identified concepts of Fake News?

As stated previously, when responding to RQ2, several key concepts in fake news are important to understand before evaluating how to tackle the problem. Now that they are identified, it's possible and necessary to analyse the relationship shared between them.

Figure 4 presented below, shows the inter-relationship between the various concepts of fake news

These relations contribute to the end product, the spread of fake news, and allow greater comprehension of what to tackle to mitigate its impact on the world.

Table 2 Identified concepts of fake news

Concept	Definition	Papers
Impact	Impact refers to the consequences of an action. As a concept of fake news, it relates to the effect that the spreading of fake news can create, both in terms of reach and in terms of damage, and therefore, must be considered when analyzing false information.	16
Verifiability	The ability to check if information is accurate and reliable, making it possible to determine news as true, false, or misleading.	8
Intent	Intent refers to the motive for creating or spreading fake news or news taken out of context. It can vary from personal gain to great campaigns to support agendas.	8
Agent	Agent refers to the person or entity that fabricates or spreads fake news. This agent may use different methods to create false information and can be driven by a personal or political agenda.	7
Source	It refers to the origin of the news, which can come from an individual, group, company, or political party. In opposition to the agent, the source may not know the information is false or misleading.	6
Medium	Medium as a concept of fake news relates to the platform or method that is used to spread false information.	6
Context	Context refers to the situation that involves a story or article. This context is essential, as news or facts taken out-of-context can lead to misleading information and the dissemination of fake news.	5
Event	Event refers to the occurrence of fake news, which may be of different types, and lead to false or misleading news being created.	3
Content	Content refers to the existing information in news that is presented as true, but is in fact false or misleading.	2
Deepfake	The term “deepfake” is a combination of “deep learning” and “fake news,” and refers to synthetic media files created using machine learning and artificial intelligence to deceive.	2
Echo Chambers	Echo chambers are settings that exist especially on social media, where users choose to interact with others and read news in ways that support their own beliefs. This process creates a positive feedback loop, where individuals are constantly exposed to information that aligns with their beliefs, leading to a subjective meaning of truth.	2
Truthiness	Truthiness refers to how the reception of an information, and its validity is based on the feeling a person gets from the information in a post-fact world. A “post-fact world” is what a person wishes it to be, independently of whether it is verifiable or not.	1

Concepts	Impact	Intent	Agent	Medium	Context	Content	DeepFake	Echo Chambers	Event	Source	Truthiness	Verifiability
Impact		trigger	rely	rely	rely	rely	rely	rely	trigger	rely	rely	exploit, rely
Intent	generate		drive	influence	—	influence	—	originate	generate, exploit	exploit	—	avoid
Agent	generate	shows		use	generate	create	create	exploit	create	exploit	exploit	avoid
Medium	Influence	—	rely		—	spread	—	exploit	—	rely	exploit	—
Context	shape, generate	generate	rely	—		induce	influence	—	generate	rely	generate	generate
Content	shape	—	rely	rely	—		—	—	rely	—	—	generate
DeepFake	generate	rely	rely	—	—	rely		exploit	rely	originate	exploit	avoid
Echo Chambers	generate	generate	generate	rely	—	—	—		—	—	generate	avoid
Event	trigger	originate	originate	rely	generate	generate	—	generate		—	generate	avoid
Source	generate	generate	—	use, rely	generate	generate spread	generate	exploit	generate, spread		exploit	—
Truthiness	generate	generate	—	—	rely	rely	—	—	—	—		disregard
Verifiability	Reduce, Generate	—	investigate	use	verify	verify	verify, disregard	—	verify, disregard	verify, disregard	influence	

Fig. 4 Inter-relationship between the identified concepts of Fake News. (Source: Author's on creation)

The information era that we live in creates an increasing ease in sharing and spreading information that may be false, and in the last years, brought new concepts such as Deepfakes, showing that not only disseminating news is easier, but fabricating them has been taken to a level unforeseen in the past. With agents having this ability to use the medium to circulate fake news, their intent impacts companies, groups, and individuals more than ever, and therefore, extra efforts in analyzing the sources and the content of news are essential. Furthermore, there are cases where, although the information shared has accurate content, it may be taken out of context. This can happen with statements and information or with simple facts and generate events that create victims due to misleading information being shared. Being able to verify the content available and the context in which it is shared reduces the impact of fake news. Other concepts, such as Echo Chambers, may contribute to biased opinions. This can not only lead to new agents with intent of misleading, but it can also lead to agents exploiting people in echo chambers to believe in something that may not be true or have unknown alternatives. Echo chambers may also lead to cases of truthiness, where people may accept news and information because they agree with the same information.

This interconnectedness creates a complex web of relationships, which assists in identifying points of intervention to reduce the risks brought on by fake news.

RQ 4 – What is the relationship between the concepts of Fake News and Digital Risk Management?

To clarify the connection between fake news and digital risk management, a comparison can be made between these concepts and existing standardization frameworks, such as the ISO 31,000 family of standards for risk management. A conceptual map for digital risk derived from existing ontologies can be used to understand the multifaceted nature of digital risk. Figure 5 highlights the interconnectedness of various elements within the digital environment and how they contribute to the complexity of managing digital risks.

With the knowledge of the digital risk concepts present in Fig. 5, together with the fake news concepts defined in RQ2, it is possible to correlate the concepts and describe the relationship between them. Fake news can be understood as a specific instance of a threat within the digital risk landscape, and therefore, the relationship of fake news with the concepts of digital risk is demonstrated in Fig. 5. However, the various concepts of fake news can interact differently with digital risk. These interactions are displayed in Figs. 6 and 7, where fake news concepts are present in the left column, and the concepts

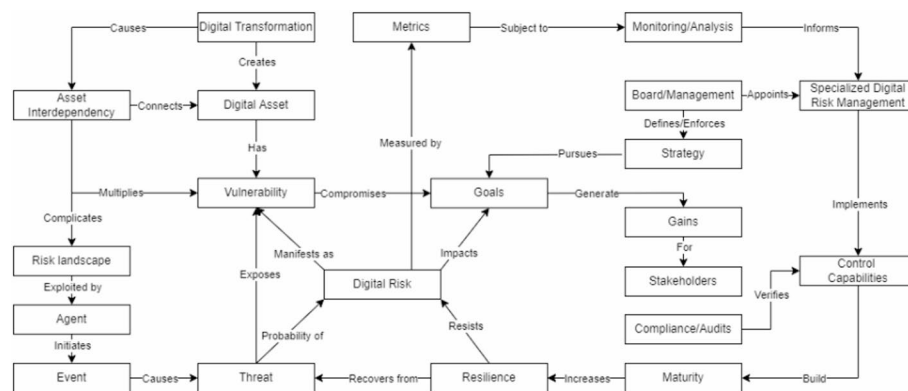


Fig. 5 Digital Risk Concepts. (Source: [34])

	Asset Interdependency	Risk Landscape	Agent	Event	Digital Transformation	Digital Asset	Vulnerability	Threat	Digital Risk	Resilience	Control Capabilities
Impact	affect	affect	rely	trigger	affect	damage	expose	cause	represent	—	—
Intent	—	—	—	—	—	—	—	generate	induce	—	—
Agent	—	exploit	represent	create	affect	threaten	expose	cause	—	affect	—
Medium	—	affect	rely	—	—	—	—	—	—	—	affect
Context	—	—	—	—	—	expose	expose	generate	—	—	—
Content	—	—	rely	—	—	expose	exploit	—	—	—	—
DeepFake	—	exploit	rely	—	—	—	exploit	generate	induce	—	—
Echo Chambers	affect	—	—	—	—	—	expose	—	—	—	—
Event	—	affect	—	—	—	affect	exploit	cause	induce	affect	—
Source	—	—	relate	create	—	—	—	promote	induce	—	—
Truthiness	—	—	—	—	—	—	expose	—	affect	—	promotes
Verifiability	—	—	—	—	—	—	—	validate	confirm	—	strengthen

Fig. 6 Relationship between fake news concepts and digital risk concepts, part 1. (Source: Author's on creation)

	Goals	Metrics	Monitoring / Analysis	Board Management	Strategy	Gains	Stakeholders	Compliance / Audits	Maturity	Specialised Digital Risk Management
Impact	influence	affects	necessitate	—	shape	affect	expose	—	—	—
Intent	drive	—	—	—	—	—	—	—	—	—
Agent	—	—	—	—	—	affect	target	—	—	—
Medium	—	affect	determine	—	—	—	—	—	—	—
Context	—	—	—	affect	endanger	affect	expose	—	—	—
Content	threaten	affect	—	—	—	—	—	—	—	—
DeepFake	—	—	complicate	—	—	—	—	—	—	—
Echo Chambers	—	—	—	—	—	—	—	—	—	—
Event	—	—	trigger	—	compromise	affect	concern	—	—	—
Source	—	—	—	—	—	—	—	—	—	—
Truthiness	—	—	—	—	—	—	—	—	—	—
Verifiability	—	—	aid	—	aid	affect	—	—	—	inform

Fig. 7 Relationship between fake news concepts and digital risk concepts, part 2. (Source: Author's on creation)

present in Fig. 5 are on the upper line. The relation between them is represented by a single verb when existent and by three dash lines when non-existent. The Figs. 6 and 7 are presented below:

The relationships depicted in Figs. 6 and 7 reveal that the various concepts of fake news interact unevenly across the digital risk landscape. While some concepts, such as impact, agent, and event, demonstrate strong and multifaceted connections with core digital risk elements, others, such as truthiness and verifiability, exhibit more focused links related to control capabilities and resilience. This differentiation highlights that fake news operates not as a singular digital threat, but as a composite phenomenon that influences and is influenced by multiple dimensions of digital risk.

Through these interactions, fake news emerges as both a catalyst and an amplifier of digital vulnerabilities. Elements like medium, context, and deepfakes contribute to the exposure and generation of threats by exploiting digital interdependencies and the

dynamics of online communication. Alternatively, concepts such as verifiability and truthiness play a stabilizing role, aligning with control and validation mechanisms that support risk mitigation and enhance organizational resilience.

Overall, the mapping demonstrates that addressing fake news within digital risk management requires a multidimensional approach that considers its technical, organizational, and social dimensions. Effective strategies must integrate continuous monitoring, information verification, and resilience-building measures to mitigate the evolving risks posed by fake news within complex digital ecosystems.

6 Discussion

This section discusses the results obtained and compares them with a systematic literature review (SLR) done on the same theme Varela [12].

The results of the MLR provide novel insights into the interplay between fake news and risk management. Firstly, the discussion on the topic requires a great study of the definition of fake news, and this study shows that there are various definitions for fake news, meaning that both authors and society as a whole may use the definitions found in the articles as well as other possible definitions that weren't present to refer to fake news. From the articles chosen, it is clear that the terms used to define fake news, occasionally used as synonyms, have their differences.

In response to the second research question, the prominence of Impact highlights its centrality in the topic, with authors repeatedly emphasizing the real-world consequences of fake news. The SLR similarly identifies Impact as a critical theme. The frequency of the concepts of verifiability, Agent, Source and Intent in the MLR reflects a strong emphasis on the means of fake news creation, detection and dissemination. These four concepts that reflect, respectively, the ability to determine if an information is true or false, the actor responsible for creating or spreading fake news, the origin of the news, and the motivation behind creating or spreading fake news, emerge together as a recurring concern in the rise of fake news and the capacity to distinguish true from false information. It is interesting to note that the concepts DeepFake, Echo Chambers, and Truthiness, although not appearing often in the articles researched, are absent as key concepts in the SLR research. This may happen due to the nature of the research, as new concepts may not be as present in academic research as in grey literature. The following table presents the divergences in the concepts found in the MLR and SLR Table 3.

The MLR study reveals a highly interconnected network between the fake news concepts identified, showing that the concepts are strongly intertwined. However, it's curious to note that some connections that may seem certain at first glance, such as between source and agent or between intent and deepfake, are absent from the table. This may come for different and diverse reasons. Grey literature, which is often shorter than academic work, may be too concise to grasp all the connections between the concepts of

Table 3 Divergences in the concepts found in the SLR and MLR. Source: (Author's on creation based on Varela [12])

Concept in the MLR	Concept in the SLR
Intent	Intention
Deepfake	
Echo Chambers	
Truthiness	

fake news, as most articles focus on a subsection of fake news, and not on the theme as a whole. Another reason might be that similar concepts may not appear together often.

The SLR provides an even more interconnected table Varela [12], an outcome that may be due to both the extension of the academic papers, which provides more opportunities to explore the theme fully and the more thorough work in studying the vast area and concepts of fake news.

To respond to the last research question, deeper study is required into the area of digital risk. Namely, ISO 31,000 (International Organization for Standardization [22], which states that a methodical strategy that considers the interaction between various aspects of uncertainty and their possible effects is necessary for identifying and managing risks. Fake news aligns closely with this context, as it creates uncertainty through the distortion of information. By making a parallelism between fake news and the concepts of digital risk mapped in Fig. 5 [34], fake news can be seen as a threat to digital risk, exploiting vulnerabilities in digital ecosystems, such as the algorithms of social media platforms and the ease of content virality.

However, as highlighted by [34], adopting frameworks such as ISO 31,000 in digital contexts poses several challenges, including the lack of standardized definitions, organizational resistance to integrated risk practices, and the rapid evolution of technologies that outpace traditional management structures. These limitations underline the need for continuous adaptation and interdisciplinary expertise to ensure the framework's effectiveness in managing digital risks.

The response to the last research question sees some discrepancies between the MLR and SLR, as seen in the association table between risk management ideas and false news concepts. Although significant links are found in both assessments, the SLR finds more relationships, which indicates its methodical and targeted approach to examining these intersections. In contrast, most of the articles in the MLR touch only briefly on risk management, focusing primarily on fake news itself. Some risk management concepts, such as vulnerability and threat, are still highly referred to, but most of the risk management key concepts are omitted from the articles, which focus more on the management of fake news and the possibilities for mitigating the issue.

7 Conclusion

By framing fake news as a threat to risk management, it becomes possible to approach it systematically through the principles of risk management. This perspective enables the application of established strategies to identify, assess, and mitigate the threats of fake news to organizational objectives, public safety, and societal trust. Risk management, as a structured process, provides the necessary tools and methodologies for prioritizing risks and implementing effective solutions to address them.

In this work, a Multivocal Literature Review MLR was conducted to gather insights from both academic research and grey literature, offering a comprehensive understanding of fake news and its connection to risk management. The findings from the MLR highlight the problem of tackling fake news and soliciting innovation in solutions to

reduce the consequences of the problem. This opens the path for potential solutions based on innovative ideas that can act in the prevention, mitigation or aftermath of fake news. Even though the papers studied for the MLR provide a great understanding of the theme of fake news, the articles found do not produce abundant information on the link between fake news and the concepts of digital risk. Namely, the grey literature articles focus mainly on fake news, grasping only a few concepts of risk management, which diminishes the connections present to respond to RQ4. Furthermore, the grey literature gathered during the search may be an unrepresentative sample of all unpublished papers [17].

This research provides numerous possibilities for future work, including using AI and machine learning to detect fake news more accurately, developing structured frameworks that incorporate fake news as a risk in organizational risk management strategies, or using multi-criteria decision analysis to select countermeasures to mitigate fake news.

Appendix

See Tables 4, 5, 6 and 7.

Table 4 Scientific papers accepted

Title	Author	Year	Reference
Fake News: a conceptual model for risk management	João Varela da Costa, Sílvia Bogeia Gomes, and Miguel Mira da Silva	2024	da Costa et al. [12]
Fake news, misinformation, disinformation, and supply chain risks and disruptions: risk management and resilience using blockchain	Petratos, P and Faccia, A	2023	Petratos and Faccia [32]
On how to characterize and confront misinformation in a risk context	Terje Aven and Shital A. Thekdi	2022	Aven and Thekdi [5]
Misinformation, disinformation, and fake news: Cyber risks to business	Pythagoras N. Petratos	2021	Petratos [31]
The Fake News Game: Actively Inoculating Against the Risk of Misinformation	Jon Roozenbeek, Sander van der Linden	2018	Roozenbeek and der Linden [38]
Impacts of fake news in the administrative scope: risk management in companies and impact on the financial market	Danilo Ojeda Alves, Julio Afonso Alves Dutra	2023	Ojeda Alves & Alves Dutra [29]
Role of fake news and misinformation in supply chain disruption: impact of technology competency as moderator	Sheshadri Chatterjee, Ranjan Chaudhuri, and Demetris Vrontis	2022	Chatterjee et al. [11]
How Truthiness, Fake News and Post-Fact Endanger Brands and What to Do About It	Pierre Berthon, Emily Treen, and Leyland Pitt	2018	Berthon et al. [7]

Table 5 Grey literature accepted

Title	Author	Year	Reference
The Real Risks of Fake News	Haber, Morey	2017	Haber [20]
True or false? Here are five ways to manage false information about risk	Sophie Richter	2022	Richter [36]
How to manage fake news risk	n.f.	2018	Strategic Risk [41]
Spotlight on: Fake news risks and how to tackle them	Trevor Treharne	2023	Treharne [43]
Risk Management And Misinformation Campaigns	Troy Rydman	2021	Rydman [39]
Disinformation and Deepfakes Risk Management (DDRM)	Matthew F. Ferraro, Jason C. Chipman, Jason L. Kropp, Stephen W. Preston, Louis W. Tompros	2022	Ferraro et al. [15]
The three horsemen of cyber risks: misinformation, disinformation, and fake news	Shannon Williams	2021	Williams [46]
Fake News, Real Threat	Alex Wright	2017	Wright [47]
Managing the risk of fake news	n.f.	2020	Strategic Risk [42]
Combatting Fake News	n.f.	n.a.	ISIS STFC [24]
Detection and protection in the era of “fake news”	Matt Essert	2020	Essert [14]
Fake News and Cyber Propaganda: The Use and Abuse of Social Media	Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin	2017	Gu et al. [19]
AI and Data-Powered integrated risk management	n.f.	2024	PWC [33]
Managing the risk of misinformation and fake news	n.f.	2023	IRM India [23]
Fact vs. Fake: Managing the risk of misinformation	n.f.	2023	BusinessTech [10]

Table 6 Terms for fake news referenced articles

Term	References
Misinformation	da Costa et al. [12], Strategic Risk [41], Petratos and Faccia [32], Rydman [39], Aven and Thekdi [5], Petratos [31], Williams [46], ISIS STFC [24], Essert [14], IRM India [23], Chatterjee et al. [11], BusinessTech [10], Roozenbeek and der Linden [38], Haber [20], Wright [47], Gu et al. [19]
Disinformation	da Costa et al. [12], Petratos and Faccia [32], Rydman [39], Aven and Thekdi [5], Petratos [31], Ferraro et al. [15], Williams [46], Essert [14], BusinessTech [10], Roozenbeek and der Linden [38]
False Information	da Costa et al. [12], Richter [36], Petratos and Faccia [32], Treharne [43], Petratos [31], Ferraro et al. [15], Roozenbeek and der Linden [38], Aven and Thekdi [5], Essert [14], IRM India [23]
Misleading Information	da Costa et al. [12], Richter [36], Petratos and Faccia [32], Treharne [43], Chatterjee et al. [11], Petratos [31], Aven and Thekdi [5], Williams [46], Essert [14]
Fabricated Information	da Costa et al. [12], Petratos and Faccia [32], Chatterjee et al. [11], Petratos [31]
Propaganda	da Costa et al. [12], Gu et al. [19], Petratos [31], Roozenbeek and der Linden [38]
Information Distortion	Petratos and Faccia [32]
Mal-information	Aven and Thekdi [5]

Table 7 Concepts of fake news referenced articles

Concept	References
Impact	da Costa et al. [12], Haber [20], Richter [36], Strategic Risk [41], Petratos and Faccia [32], Treharne [43], Aven and Thekdi [5], Petratos [31], Williams [46], Wright [47], ISIS STFC [24], PWC [33], IRM India [23], Ojeda Alves & Alves Dutra [29], Chatterjee et al. [11], BusinessTech [10]
Verifiability	da Costa et al. [12], Haber [20], Richter [36], Strategic Risk [41], Aven and Thekdi [5], IRM India [23], Ojeda Alves & Alves Dutra [29], Chatterjee et al. [11]
Intent	da Costa et al. [12], Richter [36], Petratos and Faccia [32], Aven and Thekdi [5], Petratos [31], IRM India [23], Ojeda Alves & Alves Dutra [29], Chatterjee et al. [11]
Agent	da Costa et al. [12], Haber [20], Aven and Thekdi [5], Ferraro et al. [15], Williams [46], Essert [14], Gu et al. [19]
Source	da Costa et al. [12], Strategic Risk [41], Aven and Thekdi [5], Roozenbeek and der Linden [38], Ojeda Alves & Alves Dutra [29], Chatterjee et al. [11]
Medium	da Costa et al. [12], Haber [20], Wright [47], ISIS STFC [24], Gu et al. [19], Berthon et al. [7]
Context	da Costa et al. [12], Haber [20], Richter [36], Strategic Risk [41], Aven and Thekdi [5]
Event	da Costa et al. [12], Treharne [43], Essert [14]
Content	da Costa et al. [12], Haber [20]
Deepfake	PWC [33], Essert [14]
Echo Chambers	Roozenbeek and der Linden [38], Berthon et al. [7]
Truthiness	Berthon et al. [7]

Acknowledgements

This work was funded by national funds through FCT - Fundação para a Ciência e a Tecnologia I.P. under the support UID/6486/2025, and partially supported by the European Union's Horizon Europe research and innovation program FERMI under the grant agreement No. 101073980.

Author contributions

EN conducted the MLR and wrote the draft of the manuscript. JVC participated in the design of the research protocol and validated the study results. MMS coordinated the study, participated in the design of the research protocol. All authors read and approved the final manuscript.

Funding

Open access funding provided by FCT|FCCN (b-on). This work was funded by national funds through FCT - Fundação para a Ciência e a Tecnologia I.P. under the support UID/6486/2025, and partially supported by the European Union's Horizon Europe research and innovation program FERMI under the grant agreement No. 101073980.

Data availability

No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate

This article does not contain any studies involving human participants performed by any of the authors.

Consent for publication

Not applicable.

Competing interests

The authors declare no competing interests.

Received: 11 June 2025 / Accepted: 31 December 2025

Published online: 12 January 2026

References

1. Aimeur E, Amri S, Brassard G. Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*. 2023;13(1):30.
2. Al-Asadi MA, Tasdemir S. (2021). Using artificial intelligence against the phenomenon of fake news: a systematic literature review. *Combating Fake News Comput Intell Techniques*, 39–54.
3. Alemanno A. How to counter fake news? A taxonomy of anti-fake news approaches. *Eur J Risk Regul*. 2018;9(1):1–5.
4. Allcott H, Gentzkow M. Social media and fake news in the 2016 election. *J Econ Perspect*. 2017;31(2):211–36.
5. Aven T, Thekdi SA. On how to characterize and confront misinformation in a risk context. *J Risk Res*. 2022;25(11–12):1272–87.
6. Bakir V, Andrew McStay. &. (2018). Fake news and the economy of emotions: Problems, causes, solutions. *Digit Journalism*, 154–75.
7. Berthon P, Treen E, Pitt L. How truthiness, fake news and post-fact endanger brands and what to do about it. *NIM Mark Intell Rev*. 2018;10(1):18–23.

8. Botha J, Pieterse H. (2020). Fake news and deepfakes: A dangerous threat for 21st century information security. *ICCWS 2020 15th International Conference on Cyber Warfare and Security. Academic Conferences and Publishing Limited*.
9. Brocal F, González C, Sebastián MA, Reniers GLL, Paltrinieri N. Standardized risk assessment techniques: a review in the framework of occupational safety. *Saf Reliability-Safe Soc Chang World*. 2018;2889:2895.
10. BusinessTech. (2023). *Fact vs. Fake: Managing the risk of misinformation*. <https://businesstech.co.za/news/industry-news/665173/fact-vs-fake-managing-the-risk-of-misinformation/>
11. Chatterjee S, Chaudhuri R, Vrontis D. Role of fake news and misinformation in supply chain disruption: impact of technology competency as moderator. *Ann Oper Res*. 2023;327(2):659–82.
12. da Costa J, Bogaes Gomes S, da Silva M. Fake news: a conceptual model for risk management. *Humanities and Social Sciences Communications*. 2024;11(1):1–11.
13. Eskander RFA. Risk assessment influencing factors for Arabian construction projects using analytic hierarchy process. *Alexandria Eng J*. 2018;57(4):4207–18.
14. Essert M. (2020). *Detection and protection in the era of fake news*. <https://digitalstrategies.tuck.dartmouth.edu/wp-content/uploads/2020/07/Matt-Essert-Deepfakes.pdf>
15. Ferraro MF, Chipman JC, Kropp JL, & others. (2022). *Disinformation and Deepfakes Risk Management (DDRM)*. https://www.wilmerhale.com/-/media/files/shared_content/editorial/publications/documents/20220429-wilmerhale-on-disinformation-and-deepfakes-risk-management.pdf
16. Figueira Á, Oliveira L. The current state of fake news: challenges and opportunities. *Procedia Comput Sci*. 2017. <https://doi.org/10.1016/j.procs.2017.11.106>.
17. Garousi V, Felderer M, Mäntylä MV. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Inf Softw Technol*. 2019. <https://doi.org/10.1016/j.infsof.2018.09.006>.
18. Gelfert A. Fake news: a definition. *Informal Log*. 2018;38(1):84–117.
19. Gu L, Kropotov V, Yarochkin F, & others. (2017). *Fake News and Cyber Propaganda: The Use and Abuse of Social Media*. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media>
20. Haber M. (2017). *The Real Risks of Fake News*. https://www.aferm.org/erm_feed/real-risks-fake-news/
21. Höchstötter N, Lewandowski D. What users see – structures in search engine results pages. *Inf Sci*. 2009. <https://doi.org/10.1016/j.ins.2009.01.028>.
22. International Organization for Standardization. (2018). *ISO 31000:2018 Risk management — Guidelines*.
23. IRM India. (2023). *Managing the risk of misinformation and fake news*. <https://www.theirmindia.org/blog/managing-the-risk-of-misinformation-and-fake-news/>
24. ISIS STFC. (2020). *Combating Fake News*. <https://www.isis.stfc.ac.uk/Pages/Themes.aspx>
25. Kirchner J, Reuter C. Countering fake news: a comparison of possible solutions regarding user acceptance and effectiveness. *Proc ACM Hum Comput Interact*. 2020;4(CSCW2):1–27.
26. Kitchenham ~ B C et al. (2007). *(Guidelines for performing systematic literature reviews in software engineering*.
27. Marshall H, Drieschova A. Post-truth politics in the UK's brexit referendum. *New Perspectives: SAGE Publications Sage UK*; 2018.
28. Mukerji N. (2018). *What is fake news?*.
29. Ojeda Alves D, Alves Dutra JA. IMPACTOS DAS FAKE NEWS NO ÂMBITO ADMINISTRATIVO: GESTÃO DE RISCO NAS EMPRESAS E REPERCUSSÃO NO MERCADO FINANCEIRO. *REVISTA FOCO*. 2023. <https://doi.org/10.54751/revistafoco.v16n6-154>.
30. Peter N. The the impact of digitalization on a companys\} risk management. *MAP Social Sciences*. 2023;3(1):41–50.
31. Petratos PN. Misinformation, disinformation, and fake news: cyber risks to business. *Bus Horiz*. 2021;64(6):763–74. <https://doi.org/10.1016/J.BUSHOR.2021.07.012>.
32. Petratos PN, Faccia A. Fake news, misinformation, disinformation and supply chain risks and disruptions: risk management and resilience using blockchain. *Ann Oper Res*. 2023;327(2):735–62.
33. PWC. (2024). *AI and Data-Powered integrated risk management*. <https://www.pwc.in/assets/pdfs/consulting/risk-consulting/ai-and-data-powered-integrated-risk-management.pdf>
34. Ramalho D, Diegues Fernandes A, da Silva M, Pereira R. (2024). Digital risk: a systematic multivocal literature review. *Inform Secur Journal: Global Perspective*, 1–21.
35. Rehacek P. Risk management standards for project management. *Int J Adv Appl Sci*. 2017;4:1–13.
36. Richter S. (2022). *True or false? Here are five ways to manage false information about risk*. <https://www.undrr.org/news/true-or-false-here-are-five-ways-manage-false-information-about-risk>
37. Rocha YM, De Moura GA, Desidério GA, De Oliveira CH, Lourenço FD, de Figueiredo Nicolette LD. The impact of fake news on social media and its influence on health during the COVID-19 pandemic: a systematic review. *J Public Health*. 2023;31(7):1007–16.
38. Roozenbeek J, der Linden S. The fake news game: actively inoculating against the risk of misinformation. *J Risk Res*. 2018;22(5):570–80.
39. Rydman T. (2021). *Risk Management And Misinformation Campaigns*. <https://www.forbes.com/councils/forbestechcouncil/2021/11/16/risk-management-and-misinformation-campaigns/>
40. Shao C, Hui P, Cui P. Tracking and characterizing the competition of fact checking and misinformation: case studies. *IEEE Access*. 2018;6:75327–41.
41. Strategic Risk. (2018). *How to manage fake news risk*. <https://www.strategic-risk-global.com/operational-risk/how-to-manage-fake-news-risk/1427750.article>
42. Strategic Risk. (2020). *Managing the risk of fake news*. <https://www.top1000funds.com/2018/04/managing-the-risk-of-fake-news/>
43. Treharne T. (2023). *Spotlight on: Fake news risks and how to tackle them*. <https://www.strategic-risk-global.com/emerging-risks/spotlight-on-fake-news-risks-and-how-to-tackle-them/1446075.article>
44. Tufchi S, Yadav A, Ahmed T. (2023). A comprehensive survey of multimodal fake news detection techniques: advances, challenges, and opportunities. *Int J Multimedia Inform Retr*.
45. da Varela Costa J, Fernandes A, da Mira Silva M. Fake news and risk management: a systematic literature review. *J Risk Res*. 2024;27:1524–63.

46. Williams S. (2021). *The three horsemen of cyber risks: misinformation, disinformation, and fake news*. <https://itbrief.co.nz/story/the-three-horsemen-of-cyber-risks-misinformation-disinformation-and-fake-news>
47. Wright A. (2017). *Fake News, Real Threat*. <https://riskandinsurance.com/fake-news-real-threat/>
48. Zhang C, Gupta A, Kauten C, Deokar AV, Qin X. Detecting fake news for reducing misinformation risks using analytics approaches. *Eur J Oper Res*. 2019;279(3):1036–52.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.