VULNERABILITIES OF DIGITAL COMMUNICATION

Jyväskylä University
School of Business and Economics

Master's Thesis

2024

Authors: Anni Äikäs & Oskari Friman
Subject: Corporate Communication
Supervisor: Vilma Luoma-aho

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

ABSTRACT

Authors Äikäs, Anni & Friman, Oskari	
Title Vulnerabilities of Digital Communication	
Subject Corporate Communication	**Type of work** Master's thesis
Date February 2024	**Number of pages** 96 + Appendices

Abstract

This thesis conducts a thorough examination of the vulnerabilities present in digital communication systems, specifically emphasizing the various risks and threats they introduce to information security, privacy, and trust. To accomplish this, the research employs systematic literature review. This method provides a multifaceted understanding of digital communication vulnerabilities. The study identifies several significant vulnerabilities within digital communication, including issues related to misinformation, disinformation, and cybersecurity threats, shedding light on their substantial impact on user trust and the dissemination of information.

Recognizing the dynamic nature of the digital technology landscape and the associated challenges in keeping pace with emerging vulnerabilities, the research emphasizes the importance of continuous inquiry and the adaptation of mitigation strategies. A key outcome of this work is the development of a detailed framework designed to comprehensively comprehend and address these vulnerabilities.

This thesis is conducted in collaboration with the #HIJACK research project, which adds real-world insights and practical approaches to enhance digital security and foster trust. Overall, this study offers valuable contributions to both academic scholarship and industry practices by providing a more understandable yet academically rigorous exploration of digital communication vulnerabilities.

Key words
Digital Communication, Vulnerabilities, Misinformation, Disinformation, Social Media Vulnerabilities, Systematic Literature Review, Digital Threats

Place of storage
Jyväskylä University Library

TIIVISTELMÄ

Tekijät
Äikäs, Anni & Friman, Oskari

Työn nimi
Vulnerabilities of Digital Communication

Oppiaine Viestinnän johtaminen	**Työn laji** Pro-Gradu
Päivämäärä Helmikuu 2024	**Sivumäärä** 96 + liitteet

Tiivistelmä

Tutkielma tarkastelee digitaalisen viestintäjärjestelmien haavoittuvuuksia sekä niiden luomia uhkia ja riskejä tietoturvalle, yksityisyydelle ja luottamukselle. Tutkimus käyttää tutkimusmenetelmänä systemaattista kirjallisuuskatsausta, jolla muodostetaan monipuolinen käsitys digitaalisen viestinnän haavoittuvuuksista. Tutkimuksessa tunnistetaan useita merkittäviä digitaalisen viestinnän haavoittuvuuksia, kuten misinformaation, disinformaation ja kyberturvallisuusuhkien ongelmat ja niiden luomat huomattavat vaikutukset viestintäpalveluiden käyttäjien luottamukseen, käyttäytymiseen sekä tiedon levittämiseen.

Digitaalisten viestintäpalvelujen dynaamisen luonteen vuoksi uusien haavoittuvuuksien tunnistaminen on vaikeaa, sillä niitä syntyy nopeasti ja paljon. Tämän vuoksi tutkimuksessa korostetaan jatkuvan haavoittuvuuksien kartoittamisen, sekä ennaltaehkäisemisen tärkeyttä. Työn keskeinen tulos on haavoittuvuusprofiilien pohjalta luotu yksityiskohtaisen kehys, jonka tarkoituksena on näiden haavoittuvuuksien kokonaisvaltainen ymmärtäminen ja ennaltaehkäisy rakentamalla resilienssiä digitaaliselle disinformaatiolle.

Tämä opinnäytetyö on tehty yhteistyössä #HIJACK-tutkimushankkeen kanssa, joka lisää reaalimaailman näkemyksiä ja käytännönläheisiä lähestymistapoja digitaalisen turvallisuuden parantamiseksi ja luottamuksen edistämiseksi. Tämä tutkimus tarjoaa arvokasta näkemystä sekä akateemiseen oppineisuuteen että alan käytäntöihin, tarjoamalla ymmärrettävämmän mutta akateemisen tutkimuksen digitaalisen viestinnän haavoittuvuuksista.

Asiasanat
digitaalinen viestintä, haavoittuvuudet, misinformaatio, disinformaatio, sosiaalisen median haavoittuvuudet, systemaattinen kirjallisuuskatsaus, digitaaliset uhat

Säilytyspaikka
Jyväskyän Yliopiston Kirjasto

CONTENTS

LIST OF TABLES AND FIGURES

1 INTRODUCTION

The continual evolution of the communications field is heavily influenced by the process of digitalization. Emerging digital technologies serve as catalysts and fundamental elements in the swift overhaul of communication departments and agencies (Brockhaus, 2022). Fuelled by the internet and social media, phenomena such as misinformation, disinformation and fake news have flourished, perpetuating an environment where the distortion of facts and the dissemination of false or misleading information thrive. As per the World Economic Forum (2024), dis- and misinformation will be the most severe global risk over the next two years, as foreign and domestic actors can widen societal and political divides. Additionally, algorithms play a pivotal role in shaping the digital information landscape, influencing what content is displayed and what is obscured, thereby giving rise to filter bubbles and echo chambers (Rhodes, 2021). Thus, the current state of information is highly susceptible to misuse (Pamment, 2018), and the domain contains numerous unidentified vulnerabilities, which is what this paper aims to shed light on.

From the fields of medicine, sociology, and nursing science, vulnerability is initially approached through the lens of physical harm susceptibility, then expanded to include social vulnerability—comprising economic hardship, cultural factors, ethical responsibility, absence of protective measures, and lack of awareness or knowledge. Additionally, the concept is broadened to "situations of vulnerability," emphasizing dynamic and evolving circumstances where individuals face multiple challenges, potentially exacerbating harm or adverse consequences (Lee & Scanlon, 2007; Williams & Webb, 2021; Levasseur et al., 2020). In communication, vulnerability is dissected further into categories such as Media System Vulnerability, Public Opinion Vulnerability, and Cognitive Vulnerability, highlighting the complexities at the intersection of strategic communication and information technology. These categories reflect the difficulties in information verification, the manipulation potential of public opinion, and the influence of cognitive biases (Pamment, 2018; Hansson et al., 2020).

Scholars in corporate communications and public relations have researched the impact of digitalization on communication, focusing on digital tools like social media, websites, and intranets. The research done spans three main areas: general use of digital technologies for stakeholder relations, emphasis on social media platforms and tactics, and examination of big data, automation, and artificial intelligence. The studies explore both the potential benefits and challenges of digitalization, including cyber-attacks and data fraud. A subset of critical studies questions the effectiveness of social media and artificial intelligence for publics, organisations, and public relations. (Brockhaus, 2022.) Even though the widespread use, as well as misuse, of digital technologies for communication by organisations, their stakeholders, and society at large, has resulted in a variety of academic communication methods, procedures, and practices (Luoma-aho & Badham, 2023), the field lacks comprehensive definitions for vulnerabilities such phenomena exploit on.

The absence of a structured framework for identifying vulnerabilities in digital communication underscores the necessity for a systematic review. This review aims to integrate existing literature, providing a comprehensive understanding of the nature, risk factors, and implications of digital communication vulnerabilities across diverse domains. Weeks and Gil de Zúniga (2021, p. 279) have underscored the prevalence of misleading information and its potential impact on individuals, emphasising the importance of discerning the audience exposed to such misinformation, its occurrence locations, and its potential effects. Addressing this concern, the present study endeavours to contribute to the existing knowledge. Additionally, Chadwick and Stanyer (2022) have highlighted the lack of studies investigating the mechanisms and extent of deception in online environments—a critical concern in contemporary times. Consequently, this master's thesis aims to conduct qualitative research on the vulnerabilities inherent in digital communication, guided by the following research questions:

RQ1: In what ways can digital communication be vulnerable?

RQ2: What framework can be employed to define and categorise vulnerabilities of digital communication?

The structure of this study unfolds in the following manner: Initially, key terms are defined. The concept of digital communication is briefly introduced, and a comprehensive exploration of the term “vulnerability” and related terminology is undertaken. This thorough examination serves to establish the foundational framework for the objectives pursued in this thesis. Second, the study outlines its methodological choices and elucidates the steps involved in the research process. Third, the findings are meticulously examined and interpreted. In the fourth stage, a framework for identifying and classifying vulnerabilities in digital communication is proposed, drawing on a systematic review of the literature and additional academic contributions. After discussing the development of this framework, the final version is presented. Finally, the study concludes by discussing implications at both theoretical and managerial levels, along with providing recommendations for future research.

The artificial intelligence application ChatGPT was utilised for this paper in context to idea generation, paraphrasing, language verification in the research, and grammar correction.

2 DEFINING KEY TERMS

2.1 Digital Communication

The shift from analog technologies, such as snail mail and telephone calls, to digital counterparts like email, chat, and social media has been a fundamental aspect of digitalization in both work and leisure domains (Bloomberg, 2018, p. 3). Consequently, digital communication has played an increasingly prominent role in facilitating these transformed modes of interaction.

To delve deeper into the term, it is helpful to deconstruct it. According to The Oxford English Dictionary (2023a), "digital" is typically contrasted with analogue. As a noun, it refers to a device utilizing digital technology, and as an adjective, it pertains to numerical digits—specifically zeros and ones—employed in representing data within the realms of computing and electronics. Communication involves the conveyance and reception of messages or information, as well as the generation and duplication of meanings or understandings (Hansson et al., 2020). Therefore, digital communication can be defined as the exchange of information, data, or messages using digital technologies and electronic devices.

In the context of digital stakeholder communication, the use of both internal digital platforms (websites, intranets, mobile apps) and external platforms (Twitter, Facebook, LinkedIn, Instagram) are involved. This implies that digitized stakeholder communications can leverage two types of platforms or channels: owned media controlled by organizations, which are more challenging and expensive to maintain but offer greater differentiation and competitive advantage; and external media provided by third parties, which are generally more affordable and easier to implement but may have limited features and can be used by competitors as well. This dimension also includes the provision of digital tools for managing communication processes, constituting a core functional digital infrastructure. (Brockhaus, 2022).

2.2 Vulnerability

When investigating the lack of a definitive characterization of vulnerability in the context of digital communication, it is crucial to commence the research by referring to existing definitions established in other academic domains in depth. Vulnerability is a recognized term across numerous disciplines, unlike its synonyms and other related terms, which is why this study opted to address the subject matter using this specific term as our primary focus.

2.2.1 Definitions of Vulnerability in Different Academic Fields

The Oxford English Dictionary (2024) defines the adjective “vulnerable” as “That may be wounded; susceptible of receiving wounds or physical injury”, which initiates the term to the fields of medicine, sociology, and nursing science. While this context does not directly pertain to digital communication, it offers an initial point of reference.

In the context of Western healthcare systems physical vulnerability, as defined by Lee and Scanlon (2007), is characterized as an individual's reduced capacity to fend off further harm due to an underlying state of weakness resulting from illness, injuries, or trauma. This vulnerability, whether actualized or potential, carries the risk of exacerbating morbidity or even leading to mortality if not acknowledged or effectively addressed.

Conversely, examining how local emergency managers perceive social vulnerability, Williams and Webb (2021) identify four interconnected dimensions. Social vulnerability encompasses aspects such as economic hardship and cultural factors, the ethical responsibility to address vulnerability, the absence of protective measures, and the lack of awareness or knowledge. These categories, while distinct, are intertwined, emphasizing the complexity of social vulnerability as a multifaceted phenomenon.

In the context of older adults, vulnerability is redefined as “situations of vulnerability” by Levasseur et al. (2020). This term encapsulates a set of circumstances where, at a specific juncture, one or more individuals confront one or multiple physiological, psychological, socioeconomic, or social challenges that may interact and collectively heighten the risk of harm or adverse consequences in their lives. This definition underscores the dynamic and evolving nature of vulnerability experienced by older adults. (Levesseur et al., 2020.)

These three viewpoints on vulnerability, each rooted in unique research settings, provide intricate insights into vulnerability concerning physical well-being, societal interactions, and the specific difficulties encountered by older individuals. Together, they underscore the multifaceted nature of vulnerability and its significance across diverse academic domains such as healthcare, emergency management, and gerontology.

While these definitions emerge from separate academic domains, they are not completely isolated from the domain of digital communication. Given that digital communication and its associated vulnerabilities are inherently linked to human conduct and social contexts, there is a likelihood of significant overlap between these definitions. Therefore, it is logical to take these factors into consideration in the beginning of the research process.

TABLE 1 Vulnerability in sociology, nursing science, and medicine.

Concept as named by authors (Reference)	**Objective**	**Definition**	**Instrument of measurement**
Physical vulnerability (Lee & Scanlon, 2007) Nursing science	To define vulnerability within the context of Western health care systems	Physical vulnerability pertains to an individual's diminished ability to resist additional harm due to a weakened state resulting from illness, injuries, or trauma. This tangible or potential physical susceptibility could result in further morbidity or even mortality if not recognized or addressed.	The Acute Physiology and Chronic Health Evaluation (APACHE III) score is a method used to quantify the severity of illness in critically ill hospitalized adults, especially those in intensive care. It considers factors such as age, co-morbid conditions, and physiological and laboratory investigations conducted within the first 24 hours after admission to accurately predict hospital mortality risk or physical vulnerability.
Social vulnerability (Williams & Webb, 2021) Sociology	To understand how local emergency managers perceive and define social vulnerability.	The four ways vulnerability can be described include poverty and culture, a moral obligation, lack of security, and lack of awareness or knowledge. These categories are not completely independent of each other.	
Situational vulnerability (Levasseur et al, 2020) Medicine & Health sciences	To provide definitions of and instruments measuring vulnerability in older adults.	Based on the present research findings, it is being proposed to rename the concept as "situations of vulnerability", which can be defined as a collection of circumstances wherein, at a specific moment in time, one or more individuals experience one or multiple physiological, psychological, socioeconomic, or social challenges that may interact and contribute to an increased risk of harm or adverse impacts on their life.	The concept is best operationalized by the Perceived Vulnerability Scale (PVS). The current synthesis could aid in promoting social participation and health equity by enhancing our collective comprehension of vulnerability, including its conceptualization and measurement.

2.2.2 Vulnerability and Communication

Expanding upon a more related context, it is relevant to consider the intersections of strategic communication, as examined by Pamment (2018), and information technology, as explored by Hansson et al. (2020). In the realm of communication, vulnerabilities manifest on various levels and intersect in complex ways, affecting the exchange and understanding of information. This chapter examines the interplay and overlap of different vulnerability levels, drawing on the insights of Hansson et al. (2020) and Pamment (2018), in order to understand how they compound and contribute to the challenges posed by the rise of fake news and misinformation in contemporary media.

Pamment's (2018) work highlights three primary categories of vulnerability in communication: *Media System Vulnerability*, *Public Opinion Vulnerability*, and *Cognitive Vulnerability*. These categories emphasize challenges in the verification of information, the potential for manipulation of public opinion, and the influence of cognitive biases, all of which are crucial in addressing issues like fake news and misinformation in digital communication. *Media System Vulnerability* is underscored by the difficulties in assessing news sources, a situation exacerbated by the swift evolution of media technologies, changing patterns of media consumption, and the commercial reshaping of the media landscape. These factors exploit technological, regulatory, and economic weaknesses, paving the way for adverse influences. *Public Opinion Vulnerability* highlights the dependence of democratic societies on the discerning judgment of its citizens, a process now compromised by digital technologies that facilitate covert and anonymous engagement or impersonation in public discussions, thus undermining credible benchmarks. *Cognitive Vulnerability* refers to the natural biases and inclinations of the human mind, which are geared more towards plausibility rather than veracity. This predisposition renders individuals vulnerable to influence operations that manipulate these cognitive biases for deceptive purposes. (Pamment, 2018.)

Hansson et al.'s (2020) categorization in the context of disaster communication encompasses *Individual Vulnerability*, *Social-Structural Vulnerability*, and *Situational Vulnerability*. These categories shed light on the personal, societal, and contextual factors that can hinder effective hazard-related information exchange during crises. Addressing these dimensions is essential for enhancing disaster communication and ensuring equitable access to critical information. While these categorizations are applied to different contexts, they share common threads, especially in the realm of information dissemination and credibility.

Individual Vulnerability, as defined by Hansson et al. (2020), emerges from unique personal attributes, including physical, psychological, emotional, or behavioral traits, that limit an individual's capacity to engage with, comprehend, or respond to hazard-related information. This encompasses challenges such as cognitive, sensory, and physical disabilities, linguistic hurdles, and resource constraints. *Social-Structural Vulnerability* arises from societal disparities and the structuring of government policies that intensify these disparities, affecting the efficacy of communication infrastructures, the accessibility of information dissemination channels, and societal marginalization that fosters distrust towards authorities and media. *Situational Vulnerability pertains* to the specific circumstances of a disaster that can impede information access (for example, through the disruption of communication networks), comprehension (such as through the spread of incorrect information), and the capability to respond (like a lack of familiarity with dealing with emergencies). (Hansson et al. 2020.)

The six categories of vulnerability—Individual, Social-Structural, Situational, Media System, Public Opinion, and Cognitive—overlap in the way they contribute to the complexity of information influence and disaster risk reduction (Hansson et al., 2020; Pamment, 2018). Individual, Social-Structural, and Situational vulnerabilities underscore the personal, societal, and context-specific factors that impact disaster response and resilience. Meanwhile, Media System, Public Opinion, and Cognitive vulnerabilities highlight the susceptibility of democratic societies to misinformation and manipulation, emphasizing the role of media, public discourse, and inherent human biases. Together, these vulnerabilities illustrate the multifaceted challenges in safeguarding against misinformation and ensuring effective disaster communication and response. The table 2 below illustrates how the vulnerabilities described by Hansson (2020) and Pamment (2018) can be understood in relation to each other, emphasizing the multifaceted nature of these vulnerabilities and their potential impacts.

TABLE 2 Hansson et al. and Pamment's levels of vulnerabilities

Hansson et al. (2020)	**Pamment (2018)**	**Overlap Description**
Individual Vulnerability	Cognitive Vulnerability	Both focus on the role of individual conditions (e.g., cognitive biases) and how they can be exploited.
Social-Structural Vulnerability	Public Opinion Vulnerability	Both highlight how societal and governmental structures influence collective attitudes and can be manipulated.
Situational Vulnerability	Media System Vulnerability	Both consider the impact of specific situations or systems (e.g., media environment, disaster contexts) on vulnerability.

To conclude insights, vulnerability in the context of digital communication can be defined as the susceptibility of individuals and systems to harm or adverse consequences arising from a complex interplay of personal traits, societal disparities, and specific situational challenges. This encompasses the risks associated with misinformation, cognitive biases, and the dynamic nature of media and public discourse, highlighting the need for a nuanced understanding of how vulnerabilities impact digital communication and necessitate robust strategies for resilience and protection.

2.3 Terminology Associated with Vulnerability

In a comprehensive exploration of vulnerability characteristics, various related terms are defined to enrich the conceptual framework. These terms include liability, susceptibility, compromise, exposure, and risk.

Liability, figuratively construed, refers to an attribute or trait placing an individual at a disadvantage, presenting a burdensome factor often juxtaposed with assets (The Oxford English Dictionary, 2023b). In the context of digital communication, susceptibility to disinformation due to digital communication conditions is viewed as a liability. Susceptibility, as a quality or condition, denotes the capacity to receive, be affected by, or undergo something. In the realm of disinformation, it signifies being prone to influence, harm, or misinformation.

Compromise, as delineated by Phillips, involves putting something at risk, exposing oneself, or jeopardizing reputation, credit, or interests. This entails engaging in a hazardous course or committing to potential danger. (The Oxford English Dictionary, 2023c). In communication, compromising oneself may manifest by displaying vulnerability, such as trusting someone else and being in a susceptible state.

Exposure, broadly defined, refers to the action or state of being exposed, leaving one without shelter or defense (The Oxford English Dictionary, 2023d). Additionally, it involves subjecting or being subjected to external influence. In the context of information, exposure to disinformation or information influence signifies an undefended condition subjected to external influences.

Risk, fundamentally, involves exposure to the possibility of loss, injury, or adverse circumstances—a situation with such a possibility (The Oxford English Dictionary, 2023e). Drawing on Humpel (2006), risk transforms the uncontrollable or fate into something calculable. In communication, taking risks on security, displaying vulnerability, or choosing specific communication channels exemplifies instances where the concept of risk becomes pertinent.

TABLE 3 Terms related to vulnerability (Oxford English Dictionary)

Term	Definition	Application to communication
Liability	Figurative. An attribute or trait which sets one at a disadvantage; hence, a burdensome or disadvantageous person or thing, a handicap. Frequently opposed to assets.	Setting one at a disadvantage → Being susceptible to disinformation due to conditions of digital communication.
Susceptibility	The quality or condition of being susceptible; capability of receiving, being affected by, or undergoing something.	Susceptible to be influenced, harmed or affected by disinformation or misinformation.
Compromise	To put to the hazard of being censured' (Phillips); to expose (oneself, one's own or another's reputation, credit, or interests) to risk or danger, to imperil; to involve in a hazardous course, to commit (oneself).	Compromising oneself by showing vulnerability, in a communication setting for example, showing trust in someone else and being in a vulnerable state.
Exposure	The action of exposing; the fact or state of being exposed. The action of uncovering or leaving without shelter or defense; unsheltered or undefended condition. Also, the action of subjecting, the state or fact of being subjected to any external influence.	Undefended condition and the state of fact of being subjected to any external influence → Being exposed to disinformation or information influence.
Risk	(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility.	The general nucleus of the term 'risk' is that it turns the uncontrollable, fate, into something that can be calculated. (Humpel, 2006) For example: Engaging in communication via a certain manner, taking a risk on security, showing vulnerability etc.

2.4 Resilience

To probe the intricacies of vulnerable digital communication, it becomes imperative to establish defining parameters, thereby outlining what constitutes communication vulnerable to disinformation and what is not. The terminology employed to describe communication that demonstrates resilience, or resistance, to vulnerability is *resilient communication*. Bjola & Papadakis (2020) argue that a society can only be as resilient as its weakest, most vulnerable parts. Thus, understanding the attributes which are needed for resilience building of the public sphere to digital propaganda is the key question to answer, and also to understand why.

Resilience in communicative context can be divided into two categories, which will emerge as counters for digital propaganda (Bjola & Papadakis, 2020, p. 643). If digital propaganda is seen as a "virus" that infiltrates the information sphere of a targeted nation, it leverages the host's information mechanisms to sustain itself and reproduce. *Physical resilience* can be compared to antiviral drugs, similar to the medical approach to combating Covid-19, which doesn't eradicate the virus but hinders its growth. In contrast, *cognitive resilience* acts like a vaccine, aiming to generate sufficient defenses to ward off future viral infections (Bjola & Papadakis, 2020).

Other scholars have, on the other hand, interpreted resilience in terms of socio-psychological factors that shape individuals' response to misinformation (Comber & Grant, 2018).

As communication within the digital landscape is delved into, arriving at an unambiguous definition of resilience, which encompasses a comparison of diverse interpretations, is crucial. Tracing back to its origin, resilience is broadly portrayed as "a dynamic process where individuals display positive adaptation despite experiences of significant adversity or trauma" (Goldberg & Williams, 1988, as quoted in Haddadi & Besharat 2010, p. 1). Often conceptualized on a continuum with vulnerability, resilience implies a degree of resistance to mental health disorders without guaranteeing complete immunity from such conditions (Goldberg, 1972). In the realm of digital communication, Humprecht et al. (2023) posit that resilience manifests as a reluctance to interact with disinformation, demonstrated by refraining from sharing, liking, or commenting on such content.

2.4.1 Inoculation

A theory first introduced by William McGuire in 1964, defined as "to protect (a person or thing) from something; to make immune to the effects of something" (Oxford English Dictionary, 2023f).

Inoculation theory suggests that similar to vaccines, individuals can be prepared with mental antibodies using information. Essentially, by proactively presenting individuals with a weakened form of an opposing argument and then debunking that argument, it's possible to build resistance to future persuasive efforts on their attitudes (Roozenbeek & van der Linden, 2019)

Bjola & Papadakis (2020) argue that debunking disinformation is limited to reactive, rather than preemptive action. However, a study by Lindren et al. (2017) found out that the public can be inoculated against influential misinformation with a good success rate. In addition, the study states that, when communicating the established scientific agreement on human-induced climate change, it is advisable to include a cautionary note alerting the public to the possibility of politically or economically driven individuals trying to discredit climate science findings. Furthermore, audiences should be equipped with a fundamental understanding of disinformation campaigns to proactively counter such efforts.

As a concluding point, Roozenbeek & van der Linden (2019) argue that youth development of media literacy and education can work as the best strategy to inoculate individuals against disinformation vulnerability.

2.4.2 Trust

Trust can be defined as the act of placing belief in a statement or narrative and relying on the honesty or substantiation of an individual or their sensory perceptions. According to the Oxford English Dictionary (2023g), trust involves having confidence in the words spoken or the accounts provided by someone.

According to Hardin, (1992) trust is a perception, where you see other people trustworthy. A practical implication from this three-way relationship stands as follows: A trusts B to do X (Hardin, 1992, 154). Humans, from a very young age, balance their dependence on information on others by selectively trusting specific sources. Children show a preference for seeking and accepting information from individuals who have demonstrated accuracy in the past, rather than those who have made mistakes or admitted not knowing (Harris, 2007). Another argument for the definition of trust comes from Snijders & Keren (2001), stating that trusting is easy when there are no risks. However, when the stakes and potential risks escalate, how does this impact one's inclination to trust? The willingness to trust is influenced by individual factors, the identity of the person in question and the person to be trusted, and the particular circumstances involved (Snijders & Keren, 2001).

2.4.3 Security

According to the Oxford English Dictionary (2023h), security is defined as feeling sure or certain; free from doubt or mistrust (of something, that something is the case). Katerynych (2022) looks at security from a country perspective, stating that information security as a comprehensive security system aims to safeguard the country's interests in the information realm. This involves controlling and protecting its own domestic information sphere and ensuring the protection of its state interests in the international information space. Brooks (2010), argues that the definition of security is not a singular concept and depends on the applied context. However, a comprehensive understanding of a relevant body of security knowledge can lead to achieving a clear concept definition. Furthermore, it is suggested that security can only be defined through practical application and conceptual understanding (Brooks, 2007).

In the light of digital communication vulnerabilities, define security is hereby defined through Fischer and Green (2004, p. 21), 'security entails a steady and foreseeable setting where individuals or groups can pursue their goals without interruption or harm, free from the apprehension of potential disturbances or harm.'

2.5 Disinformation

The High Level Expert Group (2018) describes disinformation as false, inaccurate, or misleading information designed, presented, and promoted with the deliberate intent to inflict public harm or for profit. Pamment (2018) posits disinformation as a strategy that employs the distribution of false information with the intention to mislead and deceive. Lastly, Wardle (2019) defines disinformation as deliberately deceptive content crafted with harmful intent, propelled by one of three primary motivations: financial gain, exercising political influence either domestically or internationally, or merely to sow seeds of chaos.

Within the realm of information disorder, a myriad of definitions for disinformation is encountered. Our aim is to collate and present these definitions to foster a comprehensive understanding of what disinformation is and, more crucially, what it is not. According to Hansson et al. (2020), false information can assume numerous guises, ranging from satire and misleading content (classed as misinformation, which may be propagated without malintent), to manipulated or fabricated content (classified as disinformation, shared with the intent to cause harm). Other terminologies like fake news, false news, post-truth, alternative media, and so on, echo the same narrative. However, for the precision and clarity of this study, a comparative analysis of these terms has led us to adopt disinformation as our focal category. For instance, the term 'fake news' is deemed misleading, as it has been co-opted by certain politicians and their proponents to repudiate coverage they perceive as unfavorable (High Level Expert Group, 2018).

Fallis (2015) asserts that a defining attribute of disinformation, setting it apart from less detrimental forms of misleading information, is its intentional nature to deceive. This sets disinformation apart from instances of misinformation, which may arise from unintentional errors or nuanced satire.

According to Bjola & Papadakis (2020), it's increasingly agreed upon that disinformation doesn't solely depend on unconscious cognitive biases; it also necessitates the active participation of individuals in creating and spreading deceptive content.

3 METHODOLOGY

This study followed the systematic literature review approach outlined by Palmatier et al. (2017). In the phase of topic formulation, specific objectives and research questions were established to guide the review. Subsequently, procedures and methods for evaluating published works were devised to facilitate the systematic assessment process. The primary studies related to the topic were analyzed, leading to the identification of relevant keywords for constructing search strings. Given that the literature review's objective is to establish a comprehensive framework for digital communication’s vulnerabilities and, ultimately, to formulate a definition for such vulnerabilities, it was imperative to conduct a more in-depth exploration and careful selection of appropriate search terms.

Systematic reviews differ from the more usually appearing narrative reviews by adopting a replicable, scientific and transparent process, that aims to minimize bias through exhaustive literature searches of published and unpublished studies and by documenting the reviewers decisions, methodologies and ultimate conclusions (Cook, Mulrow & Haynes, 1997). Following an in-depth examination of the outcomes derived from the literature review, our subsequent step involved the formulation of a conceptual framework aimed at delineating the vulnerabilities inherent in digital communication.

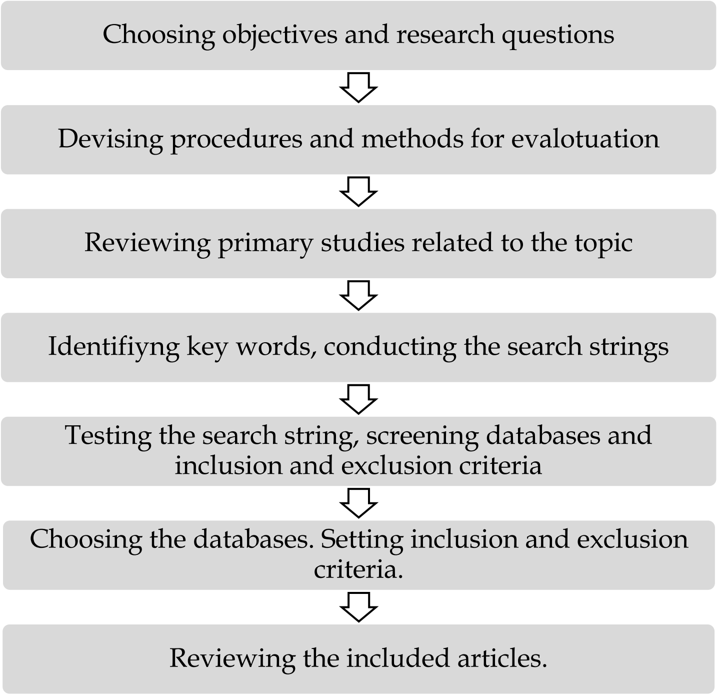

Choosing objectives and research questions
Devising procedures and methods for evalotuation
Reviewing primary studies related to the topic
Identifiyng key words, conducting the search strings
Testing the search string, screening databases and inclusion and exclusion criteria
Choosing the databases. Setting inclusion and exclusion criteria.
Reviewing the included articles.

FIGURE 1 Systematic literature reviews process (Palmatier et al., 2017)

3.1 Search string and search criteria

Following the initial screening of primary studies pertaining to the subject of communication vulnerabilities, the formulation of a structured search query was initiated. In order to complete a systematic literature review, a thorough investigation was done on the search criteria which then was tested multiple times on different databases. During the testing inclusion and exclusion criteria were established and using boolean phrases (AND, OR) the search string was developed.

The search terms were defined based on the research questions, categorizing the terms by themes. As previously articulated, vulnerability emerged as the central focal point of our investigative endeavor, accompanied by its synonymous counterparts. Synonymous expressions were characterized as embodying a pessimistic perspective, while conversely, terminology delineating dependency-oriented communication was designated to espouse a more sanguine stance. Pivotal phenomena, notably disinformation, were systematically incorporated, bearing significance within the domain of our study. Furthermore, these terminologies were contextualized within the specific investigative framework under consideration. The categorization is presented in the table below.

TABLE 4 Search string

Negative approach	Vulnerab* OR risk* OR expos* OR susceptib* OR compromis* OR liab*
Positive approach	resilien* OR secur* OR trust* OR inoculat*
Known phenomena	disinform* OR misinform* OR miscommunica*
Context	communication OR "digital communication"OR "media system*" OR "social media" OR digital

The following search string was then formed:

Vulnerab* OR risk* OR expos* OR susceptib* OR resilien* OR liab* OR compromis* OR trust OR inoculat* OR resilien* OR secur* AND disinform* OR misinform* OR communicati* OR miscommunicati* OR "digital communication" OR "media system*" OR "social media" OR digital

3.2 Search and screening criteria

The databases used in this study were restricted to the following three in order to maintain a high quality of results considering the field of study; Business Source Elite, Communication & Mass Media Complete (CMMC) and Scopus.

During our database search, specific criteria were established for the inclusion and exclusion of articles. Inclusion criteria encompassed peer-reviewed research studies of either empirical or theoretical nature, composed in English with full-text accessibility. The search was confined to articles published between 2010 and 2024.

Articles were sought by examining their titles, abstracts, and keywords. Given the initially extensive results across all databases, comprising approximately 100,000 articles, the databases were instructed to arrange the results in order of relevance. Subsequently, the top 100 articles identified as the most pertinent were chosen from each database, culminating in a total of 300 articles for subsequent scrutiny. Detailed inclusion and exclusion criteria can be found in the table below.

TABLE 5 Inclusion and exclusion criteria

Criterion	Inclusion	Exclusion
Search query	Title, abstract, keywords	All others
Study type	Peer-reviewed empirical and theoretical studies	All others
Language	English	Other languages
Source	Scholarly journals	Other sources
Availability	Full text available	Full text not available
Date	2010-2024	<2010
Relevance	100 first articles based on abstract relevance	>100 Others

TABLE 6 Practical screening inclusion and exclusion criteria

Type	Inclusion	Exclusion
Content: Title		Articles context not relevant for the review
Content: Abstract	Includes a definition, conceptualization, or detailed discussion of the attributes of digital communication that are susceptible or at risk.	
Content: Full text	Includes definitions, conceptualization, discussion, measurement tools or any relevant characterization of communication's vulnerabilities, its risk factors or such	
Content		Duplicates

A thorough evaluation of the 300 records' pertinence to our study was undertaken, involving a three-round screening procedure. In the initial round, our primary attention was directed to the titles, leading to the exclusion of records with titles that evidently lacked relevance to our research. Next, records with titles appearing pertinent were incorporated, while those with duplicate titles, or titles which did not explicitly convey relevance were held for additional assessment during the subsequent abstract review phase.

In the second round, abstracts were screened with a focus on identifying content that contained definitions, conceptualizations, or in-depth discussions regarding the attributes of digital communication prone to susceptibility or risk.

In the third round, full texts of the chosen records were assessed, with the objective of locating data pertaining to definitions, conceptualizations, discussions, measurement tools, or any relevant delineation of communication vulnerabilities, its correlated risk factors, or analogous elements contributing to the formulation of a framework for defining communication vulnerabilities. The practical inclusion and exclusion criteria used in the screening process are detailed in the table below.

In summary, the search yielded a total of 174,501 results. Given the extensive number of results, the 100 most relevant were selected articles from each database. These 300 articles were initially subjected to screening and organized into an Excel spreadsheet for subsequent evaluation. Following the eligibility assessment, **61 articles met the criteria for inclusion**, while 239 were excluded from the study.

TABLE 7 Articles included

	Scopus	**CMMC**	**Business Source Elite**
Initial search	139,662	11,196	23,643
Most relevant included	100	100	100
Excluded by title	8	29	30
Excluded by abstract	29	32	38
Excluded by full text	43	9	21
Total excluded	80	70	89
Total included	**20**	**30**	**11**

4 RESULTS

To ease the review of the 61 articles which met the criteria for inclusion, the articles were divided into groups based on the key terms provided. The conducted groups were Political Dynamics and Communication; Health Communication; Behavioral Aspects; Methods and Models in Research & Communication; Country-Specific Studies; Understanding Information Polarization, Misinformation & Disinformation; Information Management and Security; Addressing Vulnerabilities and Building Resilience; Cybersecurity and Technology; Trust in Media and News; and Social Media and Networks. The categorization was conducted according to topics and contexts, as indicated by the group names. An article can be categorized under multiple labels, facilitating the analysis of articles that investigate similar phenomena irrespective of the context, for example fake news. Additionally, this approach allows for the examination of various phenomena within the same context, for example political communication. Tables 8, 9 and 10 provide the categorized presentation of key terms along with the corresponding number of articles associated with each category.

The intent of this chapter is to go through the result articles in order to achieve an understanding of the nature of current information and research done regarding vulnerabilities of digital communication. The go-through of different themes and topics raised from the articles eases the process of deeper analysis: key variables are identified for each group. This chapter only discusses the systematic literature review's articles.

TABLE 8 Key term categories

Misinformation & Disinformation	Trust in Media and News	Methods & Models in Research and Communication	Political Dynamics and Communication	Health Communication	Country-Specific Studies
Disinformation (13) Fact-checkers Fact-checking (2) Fake news (7) Fake sources Hoax Impact of fake news on trust in news Infodemic (2) Infodemics Misinformation (9) Online disinformation Misperceptions	Broadcast meteorology Broadcast news Hybrid media environment Hybrid media system Hype news Journalism (4) Journalistic norms Journalists' survey Liberal media Media (3) Media collaboration Media cynicism Media distrust Media ownership (2) Media perceptions Media regulation (2) Media sanctions Media systems (3) Media system transformation Media transparency Media trust (5) Media use New media News consumption (2) News literacy News media (2) Press freedom Press Trust in media Trust in news Journalists' survey Media-disseminated information News audiences (2) News consumption Accuracy in journalism News agencies	Boundary work Classification Communication patterns Conceptualization Content analysis Comparative research Communication Models Communication theory Crisis communication (2) Disaster analysis Disaster risk communication Discourse theory Dual-System Theory Survey experiment Text analysis Network analysis Information adoption model (IAM) Institutional communication Risk communication (3) Technology acceptance model (TAM) Information theory Strategic communication Surveys	Citizen engagement Citizens Communication inequality Communication strategy Democracy (2) Election reporting Electoral behavior Government (2) Ideological proximity Neo-authoritarianism Oligarchization Political communication Political engagement Political misinformation Populism (2) Propaganda (2) Transitional democracy E-government services Perceived government information Transparency Political polarization	Coronavirus COVID-19 (5) COVID-19 lockdown COVID-19 pandemic COVID-19 vaccination Health communication (3) Health equity Healthcare Pandemic Public health (2) Vaccine hesitancy Lockdown (2) Global health Health care Medicine	Czech Republic Faroe Islands Ghana Africa Greenland Iceland Indonesia Italy Portugal Russia (2) Spain UAE Ukraine (2) Portuguese media system

Behavioral Aspects	Addressing vulnerabilities and Building Resilience	Understanding Information Polarization	Cybersecurity and Technology	Information Management and Security	Social Media and Networks
Fear Motivated reasoning Psychological reactance (3) Risk perception Social amplification of risk Framework Inductive reasoning Social and behavior change Social cues Social features Trust (7) Temptation and restraint Privacy Social cohesion	Credibility Inoculation (2) Resilience Risk Risk perception (2) Trustworthiness (2) Truth Truth claims Prebunking (2) Preventive inoculation Trusted execution environment Truthfulness & falsehood	Algorithmic bias Confirmation bias (2) Disconfirmation bias Echo chambers Filter bubbles Incidental exposure Selective exposure	Black-box recommender systems Blockchain Online phishing Phishing susceptibility Technology competency Side-channel attacks	Access to information Information disclosure Information environment Information security Information transparency Information warfare Information resources Security Information dissemination	Online comments social media (10) Social media platforms Social media systems Social network TikTok Mobile apps Digital media (2)

Miscellaneous	Audiences; correction (2); Culture-centered approach; Lines of differentiation; Margin of the margins (2); Natural language processing; Oz Effect; Paternalistic; power; Rebuttal; Science; Situational contingency; Stigma; User acceptance; Vladimir Putin; Youth (2); Supply chain resilience; Supply chain uncertainty; audience-media relationships; disruptive communication; race; Young students; Discussion groups; Spirituality; Polysemy; Communication; Recommender systems (2)

TABLE 9 Miscellaneous key terms

TABLE 10 Number of articles in each key term category

Category name	Number of articles
Trust in Media and News	26
Misinformation & Disinformation	22
Methods & Models in Research and Communication	20
Social Media and Networks	17
Behavioral Aspects	13
Health Communication	12
Political Dynamics and Communication	10
Addressing vulnerabilities and Building Resilience	8
Country-Specific Studies	7
Information Management and Security	7
Understanding Information Polarization	4
Cybersecurity and Technology	4
Articles with no keywords	2

4.1 Trust in Media and News

26 articles' key terms pointed them to the category of Trust in Media and News. The chapter is divided into 2 subcategories, *Journalistic responsibilities* & *Ownership,* as these were frequently emerging themes. Media has a broad range of influence on individuals, ranging from eroding trust and alternative source searching to potent trust and voting behavior. Graziano & Percoco (2016) found evidence that news media broadcasts influence people's voting behavior. News showing vast amounts of crime on television, drives people to vote for coalitions that address the crimes. Moreover, immigration news shown on television does not activate people, but crime does. This requires more research and raises a new critical question on what happens when a channel shows immigration from a crime perspective.

Koc-Michalska et al. (2023) provides more knowledge on why institutional credibility and trust is eroding. The reasons include political influencing, such as disinformation, fragmentation, polarization, dark participation and computational propaganda and micro-targeted campaigns (Freelon & Wells, 2020; Persily & Tucker, 2020). Furthermore, Chadwick (2022) studied how news stations become more vulnerable to becoming a so-called "*Trojan-horse*", who deceive the public unknowingly by changing their source practices where they use social media, online platforms, private messaging and professional media in combination. A study by Hameleers et al., (2022) suggests that skepticism towards the honesty and accuracy of the news media is diminished by the freedom of the press. Another study found that individuals lost trust in news media's intent to meet the journalistic standards in their work, after eroding trust in objectivity and accuracy of the news (Markov & Min, 2022). Trust is a difficult factor to measure as it is influenced by a number of variables. Rainear & Lachlan (2022) found that even the gender of a person affects whether individuals deem a person trustworthy, by studying broadcast meteorologists. Furthermore, it is argued that a decrease in citizens' susceptibility to attacks questioning the press's legitimacy could be achieved through a more robust and independent media, along with renewed confidence in its commitment to informing society with independence, honesty, and transparency (Hameleers et al., 2022).

Liao (2023) found that online users' perceive the news recommended to them subjectively. In order to build resilience towards online misinformation, transparent knowledge on algorithms is needed (Liao, 2023). When people lose trust in the media, they become more susceptible to disinformation. There is a reason and a rhyme, meaning that when disinformation succeeds, democratic institutions face a defeat. (Zimmermann & Kohrings, 2020). In the case study from Germany, people became skeptical of the news media and the political system through the actions of politicians and journalists who discredited themselves. Thus, leading the doubtful audience to search for alternative sources, which then expose them to disinformation. With the fall of traditional gatekeepers (see chapter 4.1.1) and declining trust for media institutions, more people are looking for alternative sources from social media (Gottfried & Shearer, 2016; Williams & Delli Carpini, 2004; Gallup, 2016). Platforms like Facebook, lacking editorial screening for false information, serve as the entry point for individuals to encounter fake news (Lazer et al., 2017; Fourney et al., 2017; Guess et al., 2017). The concept of a disinformation order arises when institutional trust erodes, giving rise to a counterforce against the existing information system (Bennet & Livingston, 2018; Rhodes, 2021).

Bauer & Clemm von Hohenberg (2021) underscores the critical role of source characteristics in shaping individuals' belief in and intention to share news reports. While there is a clear preference for real sources, even small signals from fake sources can influence people's perception. Additionally, a key finding relates to the increased belief and sharing of news reports when individuals are exposed to content congruent with their attitudes, especially for fake sources. This suggests that fake sources may exploit individuals' worldviews to build credibility quickly. This is corroborated by Sanchez & Baselga (2023), who highlight the need for regulatory measures to combat disinformation, especially in the media. While acknowledging the cognitive and epistemological dimensions of disinformation, they argue for media regulation activities to safeguard society against messages serving partisan interests. Furthermore, Splendore & Curini (2020) found that the degree of ideological proximity between individuals and journalists significantly influences trust in the media. In addition, this influence is particularly relevant for traditional media, where journalists play a more prominent role as information producers.

The study by Du (2023) illuminates how the mechanics of algorithmic news curation on social media platforms might erode trust in media. By tailoring content to user preferences, these algorithms can limit exposure to a diverse range of news sources, inadvertently fostering skepticism towards the media by creating echo chambers that reinforce existing beliefs. This dynamic underscores the need for greater transparency in how news is curated and presented, suggesting that enhancing digital literacy among consumers could be a key strategy in rebuilding trust in the media landscape. Shin (2023) introduces the concept of accuracy alerts as a mechanism to combat misinformation on social media, highlighting their potential to rebuild trust in media. By demonstrating that such alerts can decrease the likelihood of misinformation being shared, especially from algorithmic news sources, this research suggests a proactive approach to enhancing media credibility. The effectiveness of accuracy alerts in reducing misinformation dissemination underscores their value in strengthening trust between media outlets and the public, offering a strategic tool for media organizations aiming to uphold informational integrity.

According to Calvo et al. (2022) online disinformation jeopardizes a fundamental pillar of democracy – the public sphere. Study participants demonstrate limited awareness of the fact-checking phenomenon, with some perceiving it as a biased and politicized tool wielded by specific political powers. The potential of media and fact-checkers to educate emerges as a central theme. Beyond delivering quality information, they are seen as catalysts for fostering critical thinking among citizens.

BasuThakur & De (2023) highlights the heavy reliance of media on the Indian government as the primary source of information during the pandemic. This dependency resulted in a limited influence of media agenda over policy agenda, especially due to strict containment measures limiting public discourse. Furthermore, the study found out that government officials gained a trusted source status in the media as a spokesperson for continuously authenticating news items for the public. Nicoli et al. (2022) explore the opportunities blockchain technology offers in order to establish greater transparency and trust with audiences over digital communication channels. For example, it could enable social media and news media outlets to identify original sources of information in a way that is not possible at the moment.

The findings of Shi et al. (2022) on the diffusion of "*hype news*" in healthcare, particularly through endorsements by figures like Dr. Oz, offer a critical view on how reputable news outlets can sometimes amplify rather than correct misleading health information. This phenomenon underscores a significant vulnerability in digital communication, where the blend of celebrity influence and media amplification can distort public perception of health information. The slow response of academic research and marginal corrections from online customer reviews highlight the challenges in countering such misinformation, emphasizing the need for more effective oversight mechanisms in digital news dissemination to enhance public trust and discernment in media and news (Shi et al., 2022).

This chapter explored factors influencing trust in media and news, and how they contribute to susceptibility to online disinformation. When examining this group, the crucial variables to consider are the reporting actor (source characteristics) and the medium used. This involves assessing whether the report is made by a professional or a non-professional, and determining the transparency of the channels through which the information is disseminated. Establishing transparency is suggested via regulatory measures and the potential of blockchain technology.

4.1.1 Journalistic responsibilities

Acting as a facilitator, journalism is tasked with observing and monitoring to gather pertinent details about public affairs, societal conditions, trends, and concerns. In this role, journalists are responsible for disseminating crucial, accurate information to the public. It's crucial to emphasize that journalists play a significant societal role, capable of influencing public decisions, especially during times of crisis (Gálik & Tolnaiová, 2022). A study by Balod & Hameleers (2021) asks the question about journalists' role in debunking misinformation, which opens up a new discussion regarding gatekeeping, limitations and ethical responsibilities that fall on their shoulders. Journalists can face limitations in combating misinformation due to factors such as routines, deadlines, extra-media pressures, or editorial decisions, which can impede their ability to act on their perceived role of countering fake news and accusations (Tandoc et al., 2012). Russian journalists' face enormous challenges from concentrated media ownership (see chapter 4.1.2), hindering their independence and ability to work (Slavtcheva-Petkova, 2019). Journalists often struggle to verify information due to time constraints, with some newsrooms employing independent fact checkers, but ultimately it is the responsibility of journalists to filter out inaccurate information and this can be a tedious task, taking away time from pursuing other important stories (Balod & Hameleers (2021). Moreover, correcting misinformation or disinformation is crucial, especially when government officials are the source, as it can be seen as truth by the public and lead to dangerous consequences; journalists consider debunking fake news when judging the news value of a story. This, however, is not possible on digital settings, as public figures can post almost anything and everything on social media, leaving the vetting process to the social media platforms and ultimately, the readers to decide whether the information is correct or not. When inundated with vast amounts of misinformation to verify, some journalists may choose to postpone or even exclude unverifiable and debatable information to minimize the possibility of criticism. Even a single individual mistake can lead to accusations of generating fake news. Nevertheless, in some cases, information is published at the journalist's own expense, when accuracy is compromised due to the time constraints the journalists face (Balod & Hameleers, 2021).

4.1.2 Ownership

The concentration of ownership has negatively impacted local news as it has led to a significant emphasis on immediate financial gains by the "new media barons", often at the expense of high-quality civic journalism (Marwick & Lewis, n.d.).

Freedman (2018) argues that failures to tackle concentrated ownership, to regulate media tech companies, to safeguard an effective fourth estate and to nurture independent public service media combined has enabled spread of misinformation, distortion of election and undermined democratic processes. This is a serious article about the policy failures, highlighting possible vulnerabilities regular people can be exposed to in the digital environment. The failure to address monopolistic behavior in the digital sphere, combined with inadequate regulation and reliance on outdated frameworks, has allowed giant intermediaries to wield disproportionate influence over information dissemination. Slavtcheva-Petkova (2019) agrees with this finding, stating that concentrated ownership allows the biggest shareholders to intervene with the Russian media outlets like Radio Echo of Moscow and Novaya Gazeta, by creating financial problems and distorted facts regarding the events of Ukraine. While fines and regulatory actions against the media giants have been taken, the effectiveness of such measures remains uncertain without more radical interventions, such as breaking up or nationalizing the largest platforms (Freedman, 2018). However, according to Yanchenko (2023) the sanctions have worked in Ukraine, where some news channels have been excluded from the local media as they continuously broke journalistic norms in a "parasitic" manner.

4.2 Misinformation & Disinformation

22 articles’ key terms pointed them to the category of Misinformation & Disinformation. Exposure to misinformation significantly influences knowledge and attitudes about political issues, with actual exposure being a crucial predictor (Walter & Murphy, 2018). Identifying misinformation is challenging, leading some to overlook exposure, maintaining trust in the media. Conversely, misidentifying accurate information as misinformation can erode trust, underscoring the nuanced dangers online misinformation poses for individuals. This is a difficult storm to navigate, as misinformation has a tendency to remain persistent and resistant to correction after an individual has been exposed to it (Thorson, 2016).

However, one can’t exclude themself from exposure to disinformation and misinformation online completely. Boman (2023) argues that organizations should use inoculation theory to shield individuals from disinformation and misinformation online. Martínez-García & Ferrer (2023) state that the role of social media platforms (such as Facebook & WhatsApp) as conduits for the dissemination of disinformation poses a formidable challenge. In order to tackle the information disorder, Calvo et al., (2022) argues that media and fact-checkers should spend time educating the public, building media literacy and delivering quality information. This is corroborated by Bauer & Clemm von Hohenberg (2021), who found that social media platforms are a major medium for leading individuals to fake news websites through the individual algorithms that the media giants have built for consuming purposes. They suggest that platforms should teach users how sources can trick them into believing and spreading false information. Crucian (2023) agrees by stating that media literacy is the best investment people and governments can do in order to build resilience against online misinformation. On the contrary, Buchanan (2020) argues that media literacy only works with the assumption that people share fake news unintentionally.

Chadwick (2018) points out factors that make disinformation and deception more likely to succeed online. This includes a rich communication environment, stimulating purpose of engagement and the urgency of it. Furthermore, Krause (2022) argues that individuals can become vulnerable in different ways, emphasizing that policymakers should focus on a clear conceptualization of the information disorder in order to locate these vulnerabilities. Neyazi (2022) points out that the chosen medium of online communication may expose one further than others. Mena et al., (2020) state that online celebrities are considered as trustworthy sources, which is why Instagram has found to be one of the platforms used to run disinformation campaigns as social validation has provided exploitable circumstances.

The study by Shin (2023) reveals that accuracy alerts can effectively reduce the sharing of misinformation on social media, suggesting a valuable strategy for digital platforms to combat false information. By focusing on the differential impact of these alerts across news sources, the research underscores the potential of technological interventions in enhancing critical media consumption and promoting a more informed online discourse.

Nicoli et al., (2022) looks at the problem from a broader perspective, contemplating that capitalism contributes heavily to the digital communication vulnerabilities through advertising, consolidation, deregulation (see chapter 4.2.2.) and free market policies in the information system.

Farkas (2023) scrutinizes the depictions of fake news in news media. The study employed discourse theory and the concept of logic to analyze how media narratives discuss fake news. This framework helps understand how specific meanings and perspectives become prominent in media discussions. Two of the five identified logics are closely related to the global context: exteriorization and securitization. The logic of exteriorization portrays fake news as an external threat, often attributed to foreign entities. This logic raises suspicions about foreign involvement in domestic matters, potentially escalating diplomatic tensions and international conflicts. By framing the issue as external, this logic simplifies the complex aspects of fake news. Fake news is frequently securitized in media discussions, presenting it as a menace not only to individual nations but also to global security and democracy. This perspective leads to policy responses that transcend national boundaries and have significant consequences for international relations (Farkas, 2023). Furthermore, media experts emphasize their role as trustworthy sources and guardians against fake news. This concept underscores the significance of journalism in countering misinformation and emphasizes the media's role in shaping public perception and understanding of the societal dynamics that shape information consumption (Farkas, 2023).

According to Gálik & Tolnaiová (2022), the public needs the intellectual nourishment that media and journalists can deliver by truthful, precise, and meaningful information in order to do rational decision making. But unfortunately, disinformation and propaganda are oftentimes present in public figure's speech, thus underscoring the responsibility journalists carry by acting as the truthful gatekeepers of information (see chapter 4.1.1). Moreover, Hameleers et al. (2022) argue that citizens can hold the whole news media accountable for spreading disinformation. Quintanilha (2018) adds to this by saying that the EU should take initiative on creating regulations on social media against fake news, as they spread more widely and rapidly than true news online.

Wu et al. (2023) explore how digital media usage influences health misinformation beliefs, with a focus on the moderating effects of individual cognitive preferences. The study finds that traditional news sources tend to decrease misinformation beliefs, whereas social and alternative health media usage can increase them. The research highlights the significant impact of a person's need for cognition and their trust in intuition on how they are influenced by media, illustrating the intricate relationship between cognitive traits and media consumption in shaping beliefs about health misinformation.

Hwang and Jeong (2023) add a nuanced layer by illustrating how information processing behaviors—specifically information avoidance and heuristic processing—play crucial roles in the exposure to and acceptance of misinformation. This parallels discussions in the broader literature that emphasize the challenges of identifying and combating misinformation and the importance of media literacy and policy interventions (Walter & Murphy, 2018; Thorson, 2016; Boman, 2023; Martínez-García & Ferrer, 2023). Hwang and Jeong's findings that heuristic processing can increase susceptibility to misinformation underscore the need for comprehensive strategies that not only focus on media literacy, but also address the underlying cognitive processes that facilitate misinformation acceptance. This integration of psychological insights with media and information policy approaches offers a more holistic understanding of the misinformation ecosystem, contributing to the ongoing efforts to mitigate its impact on society. The research by Bean et al. (2022) on disinformation strategies by the Internet Research Agency targeting U.S. military veterans underscores the nuanced dynamics of misinformation and disinformation. Their findings emphasize the exploitation of existing societal divisions as a potent tool in disinformation campaigns, suggesting that the resilience against such tactics requires addressing the domestic vulnerabilities they exploit. This perspective enriches the discourse on vulnerabilities and resilience by highlighting the need for a more sophisticated understanding of disinformation mechanics beyond content analysis, advocating for strategies that also mitigate the societal fissures these campaigns leverage.

This chapter emphasizes the challenges of identifying and navigating misinformation. The key takeaway from is the distinct difference between misinformation and disinformation, which lies in the intent. Misinformation is disseminated without intent to deceive, whereas disinformation is spread deliberately for one's own advantage. Factors contributing to the success of disinformation, such as communication environment and medium choice, are discussed as well as the need for comprehensive strategies to address both content and underlying cognitive processes in combating misinformation.

4.3 Methods & Models in Research and Communication

A variety of methods and models have been employed to explore the intricacies of media dynamics, the distribution of information, and the perceptions of the public. Although this chapter may not introduce new data pertaining to the research questions, it organizes key concepts from 20 articles under the theme of Methods & Models in Research and Communication. Therefore, an examination of each article, highlighting their distinct research methodologies and demonstrating the diversity within the field, is required.

Studies such as Rhodes' (2021) and others have leveraged survey experiments to dissect the effects of algorithmic biases and tailored news on political misinformation credibility. These approaches underline the significant impact of digital environments on shaping public opinion. Conversely, Gongora-Svartzman and Ramirez-Marquez (2022) represent research harnessing text processing and network analysis. Their work underscores the pivotal role of social media in community resilience during crises, showcasing strategic communication benefits. The studies by Ravn-Højgaard et al. (2021) and Maloney et al. (2024) utilize comparative and content analysis to explore the operation of media systems and the media's portrayal of events like the COVID-19 pandemic. These methodologies offer insights into the influence of local factors and media biases. Additionally, Yanchenko et al. (2023) and Farkas (2023) adopt thematic and qualitative analysis to delve into the discourse around journalistic legitimacy and the construction of "fake news" as a security issue, respectively, highlighting the nuanced understanding of media narratives. Balaskas et al. (2022) and Bearth & Siegrist (2022) apply structural equation modelling and the Social Amplification of Risk Framework, respectively. Their work integrates trust, technology acceptance, and a positive perspective in risk communication, offering comprehensive models for evaluating communication effectiveness. Sánchez and Villanueva Baselga (2023) and Hwang and Jeong (2023) emphasize the role of cognitive biases and psychological dimensions in processing information. These studies suggest expanding traditional frameworks to include behavioral insights in misinformation analysis. Baptista (2022) focuses on the Media Pluralism Monitor's application in assessing transparency and accountability within media entities. This research highlights the dual aspects of transparency—upward and downward—and their significance in informed decision-making.

The array of methodologies from survey experiments to structural equation modelling illustrates the depth and diversity of approaches in communication research. Each method provides unique insights, contributing to a comprehensive understanding of the media's complex role in society.

4.4 Social Media and Networks

17 articles were pointed to the group of Social Media and Networks. These articles collectively highlight vulnerabilities of digital communication on social media, such as misinformation, political polarization, trust erosion, and susceptibility to phishing attacks. They emphasize the challenges posed by social media in contexts like political campaigning, disaster communication, health crises, and news dissemination. The studies reveal how social media can amplify misinformation, impact political perceptions, and affect public trust in institutions. These contexts and vulnerabilities within are discussed as groups of their own, as this chapter aims to discuss the specific role social media possesses, as per 2016 62% of adults in the U.S got news from social media, and 18% reported to do so continuously (Gottfried & Shearer, 2016).

Koc-Michalska (2023) and Stubenvoll (2021) focus on how social media can propagate misinformation and disinformation. Stubenvoll (2021) underscores the interplay among social media usage, perceptions of misinformation, and trust in the media. It reveals that both political knowledge and partisanship play a substantial role in shaping these perceptions and their consequent effect on the trust placed in media sources. Koc-Michalska (2023) examines the role of social media algorithms in influencing public opinion. It is noted that these algorithms curate content in a way that often reinforces pre-existing. Molina (2023) argues that human behavior is mostly responsible for online disinformation spread. However, it is crucial to recognize the underlying platform enabling these algorithms is social media itself, which serves as a critical foundation for their operation and impact. Social media's design encourages user interaction, which can spread information rapidly, regardless of its accuracy (Heiss, 2019). Social media's design enhances user interaction through features that promote active engagement. This design strategy, which includes elements like likes, shares, comments, and personalized feeds, aims to create an environment where users are not just passive consumers of content but active participants. This participatory nature of social media facilitates rapid information dissemination and amplifies user engagement with content, contributing significantly to the spread of both accurate and inaccurate information across networks. Heiss (2019) underscores the complexity of journalistic practices in the digital age and their impact on political discourse and public opinion.

Stubenvoll (2021) marks an initial exploration into the factors preceding perceptions of misinformation and their impact on public trust in the media. The findings suggest that these perceptions contribute to a decline in trust in traditional media, with a more pronounced effect on individuals possessing limited knowledge. Additionally, robust partisan inclinations play a key role in shaping misinformation perceptions within politically engaged networks. Moreover, it is plausible to infer that individuals in these networks often encounter perceived misinformation exposure (PME), leading to diminished trust in mainstream media and an increased likelihood of seeking information from alternative sources. Consequently, as it is shown later on in this study, this action is one of the main ways to expose oneself to more misinformation & disinformation online (Rhodes, 2021).

The ease of access to social media allows for widespread dissemination of information, making it a vital tool in communication strategies (Yudarwati, 2021). The research suggests that the collectivist culture of Indonesian communities impacts the effectiveness of social media for disaster risk communication, emphasizing the importance of integrating cultural and social factors to build trust and overcome digital inequalities (Yudarwati, 2021). Neyazi (2022) highlights the complex interplay of different communication modes in spreading misinformation in a less digitalized society. The research finds that exposure to misinformation is influenced by the use of WhatsApp and Instagram for political information, while traditional media and interpersonal discussions also play significant roles. Furthermore, identifying that while social media platforms are increasingly utilized for risk communication, they present several challenges. Challenges such issues related to trust and credibility, the spread of misinformation, and digital inequality potentially hinder the effectiveness of social media as a tool for conveying critical information about risks (Neyazi, 2022). This is corroborated by Poch-Butler et al., (2023) who found that the lack of World Health Organization's responses to online disinformation in their own posts on Twitter amplifies individuals' exposure to disinformation, and more importantly, declines the possibility for corrections.

Another study by Qahri-Saremi & Turel (2023) (see chapter 4.12) investigated the social media phishing susceptibility. Social media platforms have become a breeding ground for phishing attacks, extending beyond the realms of mainstream platforms like LinkedIn and Instagram to infiltrate online dating applications (Phislabs, 2022). This evolving trend prompts an exploration into the multifaceted factors influencing susceptibility, particularly the interplay between source likability, online ostracism, and the fear-of-missing-out (FOMO) experience (Qahri-Saremi & Turel, 2023). The research delves into the pivotal role of source likability and its correlation with online ostracism, unravelling the underlying reasons behind the surge in social media phishing attacks within online dating platforms. The heightened significance of likability in these applications, coupled with the potential for increased feelings of online ostracism in the absence of attention, creates an environment conducive to successful phishing attacks. Techniques such as "ghosting" and "breadcrumbing" further exacerbate the sense of online ostracism, as revealed by recent studies (Navarro et. al., 2020), thereby amplifying susceptibility to social media phishing. Moreover, the study posits an intriguing extension of these findings by examining the impact of the fear-of-missing-out (FOMO) experience on social media phishing susceptibility. FOMO, characterized by the perception of others engaging in rewarding experiences while one is absent (James et. al., 2017), emerges as a significant antecedent of online ostracism (Holte et. al., 2022). Consequently, situations where FOMO contributes to a sense of online ostracism may weaken users' restraints against phishing messages, ultimately heightening susceptibility to social media phishing attacks (Qahri-Saremi & Turel, 2023).

Moreover, Liao (2023) adds that individuals’ perception of news algorithms and evaluation are enabled by triggering specific heuristics. For example, social belonging and acceptance online had a major significance when discussing politics.

The research by Li & Shin (2023) provides insight into the critical issue of e-cigarette misinformation on social media, demonstrating how such false information influences smokers' behavior in the UAE. It highlights the significance of source credibility in the effective correction of misinformation and suggests that addressing misinformation through credible sources is crucial in altering health-related behaviors on social platforms. This addition emphasizes the need for rigorous strategies in combating health misinformation and the pivotal role of trustworthy information sources on social media.

Crucian’s (2023) study on young students susceptibility to online disinformation found that despite their lack of awareness of "side reading" ("*The habit of checking a text as you read it, without waiting until you get to the end so as not to be influenced by it*" (Anti-Fake, 2022)), students exhibit information-checking techniques, including evaluating source credibility, author profiles, and grammatical accuracy, and demonstrate the ability to overcome certain cognitive biases during the verification process. In the study, real profile students are inclined to search for information that aligns with their existing beliefs, helping them alleviate the discomfort caused by "cognitive dissonance" more than human profile students. Nevertheless, the former group finds it more challenging to alter their opinions when influenced by a social group compared to the latter. Moreover, existing literature identifies specific demographics, such as rural residents, young people, the elderly, individuals with disabilities, and the less educated, as particularly vulnerable to disinformation. (Crucian, 2023.)

Mensah (2023) highlights that the perceived transparency of online government information plays a crucial moderating role, positively impacting the adoption of COVID-19 information. The results underscore the importance of transparent and reliable communication during pandemics to establish public trust and effectively counteract the spread of online misinformation. Conversely, Maloney et al. (2023) showed that the chosen medium for news consumption correlates with the amount of misinformation individuals are exposed to. The study also spoke about how different news stations contribute to exposing individuals to misinformation by broadcasting news containing misinformation but fail to correct the news later on as the misinformation is spotted. For example, U.S. Based news channels like CNN and MSNBC discuss misinformation more frequently than network news, with FOX also acknowledging it but without referencing President Trump as a source of misinformation regarding Covid-19. Notably, FOX includes more uncorrected misinformation statements than the two previously mentioned. Omitting misinformation disclaimers can have a significant contribution to how individuals' biases are activated by consuming news filled with misinformation (Maloney et al., 2023).

A recent study on social media use in Spain challenges the common perception of online environments perpetuating ideological echo chambers. The research reveals a moderation of selective exposure, particularly in comparison to offline media consumption. Contrary to expectations, social media users in Spain show increased exposure to diverse political and ideological views. The study emphasizes platform-specific differences, noting that Facebook tends to connect users with similar ideological positions, while Twitter provides access to both dissenting and consenting information. This distinction underscores the impact of algorithms and network dynamics in shaping users' exposure on social media platforms (Masip, 2020).

The study by Hwang and Jeong (2023) delves into the complexities of misinformation exposure and acceptance on social media, focusing on the nuances of information seeking and processing behaviors. Their research reveals that information avoidance and heuristic processing significantly contribute to the susceptibility to misinformation, underscoring the critical need for strategies that address these cognitive tendencies. The insights by Wu et al. (2023) augment the discussion on social media and networks by dissecting the relationship between media consumption and health misinformation beliefs. This study emphasizes the role of cognitive traits in mediating the impact of digital media on misinformation, offering a critical lens through which to examine the spread and acceptance of health misinformation on social platforms.

Moreover, Du (2023) explores the double-edged sword of algorithmic news personalization in social media, emphasizing its role in shaping user experiences and knowledge. While algorithms facilitate tailored content delivery, enhancing user engagement, they also risk reinforcing echo chambers and limiting exposure to diverse perspectives. This study calls attention to the importance of algorithmic transparency and digital literacy as crucial interventions to counteract the polarization and misinformation challenges inherent in social media networks.

This chapter investigated social media's role in disseminating misinformation, influencing political perceptions, and eroding trust in institutions. A critical factor in the discourse on social media and networks is the aspect of regulation: specifically, whether these channels are subject to regulatory oversight or not.

4.5 Behavioral Aspects

13 articles' key terms pointed them to the category of Behavioral Aspects. The influx of information, both from credible and non-credible sources, leads to information stress and exacerbates information overload for recipients. According to Sanchez & Baselga (2023), confirmation bias impedes the progress of acquiring knowledge about reality and obstructs the creation of a shared foundation for debating and reaching consensus on contentious matters. The biological constraints on cognitive capacity make it challenging for individuals to effectively evaluate and process the vast amount of information coming their way, whether it's from professional or non-professional media outlets. It's difficult for people to keep up with the speed and volume of information inundating them (Gálik & Tolnaiová, 2022).

A recent study by Boman (2023) studied how organizations can use inoculation theory in order to overcome the damage that a PR disinformation attack can cause. The study aimed to increase the potency of inoculation messages in order to influence people's cognitive and affective responses. By including autonomy support and specific details into the inoculation messages, psychological reactance was triggered within people's minds, fortifying the resistance to disinformation attacks. Furthermore, this then influenced people's attitudes and future behavioral intentions regarding the attacked organization. Boman (2023) continues to state that a big portion of the literature's psychological reactance focuses on reducing the motivational response, whereas this study examined how inoculation can induce reactance to stomp persuasive disinformation attempts. The study revealed that the combination of inoculation mechanisms with the induction of psychological reactance yielded better results compared to both not delivering a message and using a conventional inoculation message, as indicated by C. H. Miller et al. (2013). This observation implies that the effectiveness of traditional inoculation messages, commonly discussed in persuasion literature, can be enhanced by adjusting the control of message language.

Moussa, Radwan & Zaid (2022) studied how the level of trust young people in the United Arab Emirates have in mainstream media and government institutions impacts their ability to withstand misinformation related to COVID-19. It also examines the intricate influence of digital news literacy, along with various demographic and cultural factors, on these young individuals' attitudes regarding COVID-19 misinformation. The participants illustrated that trust is a dynamic process, where they engage in verifying information through multiple means, such as cross-checking sources and peer communication. Results from this study suggest that age group, nationality and educational major can play a significant role in misinformation perception. The study calls for the need for media literacy education.

MacKay et al.'s (2023) study focusing on Covid-19 vaccine hesitancy and its relationship with trust found out that not using the key elements of crisis communication, (transparency, targeting and tailoring information) will erode trust among people and add to their misinformation vulnerability. Moreover, if officials send out a "one-size-fits-all" message regarding Covid-19 vaccine, stating its security and effectiveness, they accidentally create skepticism and distrust towards themselves (MacKay et al., 2023). Thus, creating the "need" for the participants to conduct their own research online, as the official communication did not meet their needs nor addressed their concerns. This led the participants open for alternative messages and sources, which works towards integrity piercing vulnerability online. The conclusions of the study highlight that crisis information should be made to meet the needs and values of individuals, rather than a "one-size-fits-all" approach. (MacKay et al., 2023.)

Trustworthiness in media is affected by a magnitude of factors. Bearth & Siegrist (2022), argue that people tend to trust communication on social media more than official sources because of increased visibility of trust factors like shared values and familiarity. Moreover, social cues (such as likes) affect positively on peoples' social perception of a website as trustworthy, rather than untrustworthy (Zalmanson, Oestreicher-Singer & Ecker, 2022). Rainear & Lachan (2022) studied weather forecasters' race, gender and socio-economic status in order to find out if they gain more trustworthy status among information recipients, concluding that gender is a significant factor. In addition, the way a message is delivered has a further effect on trustworthiness.

In this informational environment, sources that lack necessary expertise and may not have the best interests of the audience at heart can gain trust. However, the challenge lies in distinguishing which sources have vested interests or disseminate false information. This challenge arises due to the inherent uncertainty associated with risk and variations in how individuals perceive and accept risks. However, Acquisti et al. (2015) argue that individuals' actions related to privacy in certain circumstances should not be seen as a direct reflection of their overall privacy beliefs. In other words, someone might have a strong general concern for privacy, but their specific choices about sharing information can be swayed by the particular costs and benefits involved in a given situation. This finding is corroborated by multiple sources. Zalmanson, Oestreicher-Singer & Ecker (2022), agree with this idea, stating that decisions regarding information disclosure are subject to influence, while broader privacy concerns tend to be more steadfast and resistant to manipulation. Wu et al., (2023) investigated misinformation susceptibility, concluding that cognitive involvement is a key factor in individuals' information processing, arguing that faith in intuition is associated with susceptibility to misinformation online. If a person is seeing higher curing potential in alternative medicine for oneself, they will go for it regardless of the misinformation (Wu et al., 2023). In addition, Paisana et al. (2020) reveal that individuals' sociodemographic variables, such as school attainment, influence their news consumption habits and perceptions of content legitimacy. Lower news literacy is linked to higher trust in social media news content, and more critically empowered consumers express greater concern about the truthfulness of digital content. Bean et al., (2022) explored Russian disinformation, concluding that exposure doesn't necessarily mean influence or impact, thus people should focus on analyzing the rhetorics of a message, regardless of origin, to discern their impact on emotions and national security perceptions.

By understanding how individuals' tendencies towards heuristic processing and information avoidance contribute to misinformation susceptibility, the challenges of information overload and stress can be addressed better. This addition underscores the necessity of fostering critical thinking and digital literacy to combat misinformation effectively, enhancing the resilience of individuals in navigating the digital information landscape. (Hwang & Jeong, 2023). Similar note is made by Sanchez & Baselga (2023), who emphasize the importance of social conditions as preventive measures towards disinformation.

Qahri-Saremi & Turel (2023), focuses on Temptation and Restraint (TR) model that explains social media phishing susceptibility as a battle between users' temptation to engage with phishing messages and their cognitive and behavioral restraint against it. The research identifies four situational factors affecting this balance: poor sleep, social media ostracism, source likability, and fear appeals. The results indicated that each of the four situational factors changes how cognitive and behavioral restraint impact susceptibility to social media phishing. The scholars argue that users typically experience an immediate gratification from checking new messages as this satisfies their curiosity (Moody, 2011). Over time, individuals form a mental link between seeing a new message and the pleasure of interacting with it. This connection triggers an irresistible urge when a new notification pops up on social media. Consequently, these urges create a strong impulse to immediately check and respond to unread messages, even if it involves risky actions (Eyal, 2014. Milyavskaya, 2015. Turel & Qahri-Saremi, 2016). However, sometimes individuals can control their impulses and limit actions that might not be the best or could pose risks. The strength of this restraint relies on two main aspects—their *motivation* and *ability* to control the urge and oppose the actions it requires (Eyal, 2014). The motivation to restrain the temptation involves users being mindful of and worried about the potential outcomes of the actions prompted by the urge. This relies on how much conflict users perceive between the likely consequences of these actions and their long-term objectives and welfare (Milyavskaya, 2015). The ability to control the urge aligns with the idea of "willpower" and demonstrates the resolve and self-control that empower users to manage the urge and counteract its impulses despite the difficulty involved (Baumeister, 2002). Users who possess both the motivation and capability to control their urge and resist the risky action it demands can restrain the action through two mechanisms (Collins, 1992). These mechanisms are *behavioral restraint* and *cognitive restraint*, which the authors correctly hypothesized to reduce one's social media phishing susceptibility if strong enough.

The key takeaway from these articles is the distinction between communication driven by emotion and logic and their contributions to resiliency and susceptibility towards online disinformation. This is evidenced by the Temptation & Restraint model, the inoculation theory, the role of trust in media and institutions in shaping attitudes to misinformation, and the influence of social media on perceptions of trustworthiness. Multiple sources suggest that privacy beliefs don't always align with specific choices about information disclosure. These studies collectively underscore the complex interplay between cognitive capacity, emotional responses, and the credibility of information sources in the digital landscape.

4.6 Health Communication

13 articles' key terms pointed them to the category of Health Communication.

The past years with Covid-19 pandemic have shown that the digital landscape can be filled with information overhaul in a matter of minutes. People have had trouble identifying reliable information sources and many ended up receiving misinformation on social media. Calvo & Valera-Ordaz (2022) and MacKay et al. (2023) converge in highlighting the perilous perception of disinformation as a formidable threat during the Covid19 pandemic. This shared concern underscores the critical role of information veracity in times of crisis. Citizens, as revealed by Calvo & Valera-Ordaz, grapple with the recognition of disinformation as a potent adversary, reflecting a vulnerability in their ability to navigate the complex information landscape effectively. MacKay et al. (2023), in their focus on vaccine hesitancy, bring to the fore the susceptibility of individuals to misinformation, reflecting the vulnerability of public trust in crucial health information.

Schiavo et al., (2022) adds that trust is increasingly challenged by the proliferation of misinformation, not only on social media but also in communities. This erosion of trust is described as a global issue that predates the COVID-19 pandemic and is linked to health, racial, and social disparities. Furthermore, the effect of misinformation on people's health is discussed as alarming and dangerous examples were heard from the President of the United States during the pandemic, referring to injecting bleach (Schiavo et al., 2022). This is further studied by Shi et al. (2022), who found out that celebrity doctors who post hyped information about health products online, influence the publicly available health information, lead consumers to make misleading conclusions. The study calls for better monitoring and control of information propagators, which will be discussed in depth during the analysis.

Trust, a central theme emerging from these articles, embodies a vulnerability that transcends national borders and demographics. Martínez-García & Ferrer (2023) divulge how distrust in institutions exacerbated political crises during the pandemic, shedding light on the fragility of public trust in governing bodies. The health crisis in Ibero-America transformed into a political crisis, as governments lacked transparency as information sources, politicians and public figures disseminated information without a scientific basis, disinformation undermined the leadership of governments and institutions, and politicians undermined the credibility of the press. Moussa, Radwan & Zaid (2022)'s findings further accentuate this vulnerability, elucidating that trust in government and mainstream media among the youth in the UAE does not necessarily correlate with their perception of COVID-19 misinformation. Meanwhile, MacKay et al. (2023) unearths the erosion of trust stemming from inadequate crisis communication. This pervasive vulnerability encompasses trust not only in information sources but also in institutions, challenging the foundations of societal resilience during crises.

Gálik & Tolnaiová (2022) and Crucian (2023) pivot towards the role of media and journalism in the context of vulnerability. Gálik & Tolnaiová emphasize the pivotal role journalism plays in quelling fear and panic during crises, underscoring the responsibility vested in media outlets and journalists. In contrast, Crucian explores the vulnerability arising from information-checking techniques among young students. These students, navigating the turbulent sea of misinformation, employ diverse strategies, but their susceptibility to the confirmation bias remains a vulnerability that warrants attention. Hwang (2023) probes information-seeking behaviors, exposing the vulnerability of selective information avoidance. Finally, Poch-Butler (2023) assesses the effectiveness of crisis communication by international organizations, revealing vulnerabilities in creating a meaningful dialogic space.

Elers et al. (2023) bring to light the vulnerability of marginalized communities in accessing information during crises, revealing a stark digital divide. Basu-Thakur (2023) explores the communication strategies adopted by governments, while Sun (2023) examines the impact of online comments on vaccination attitudes, illustrating the vulnerability of public perceptions to digital discourse. Mensah et al. (2023) highlight the critical role of transparent government communication in building trust, alleviating fears, and promoting constructive behaviors during a pandemic. The study utilizes Information Adoption Model (IAM) in order to investigate how perceived government information transparency influences the adoption of COVID-19 information on social media, and how to combat pandemic-related disinformation.

In the broader context of digital communication, these articles collectively underscore the myriad challenges that have arisen in the digital age. Crisis communication, a recurring theme, emerges as a critical aspect of managing vulnerability during a pandemic. Effective strategies adopted by governments and health organizations are paramount in shaping public perceptions and behaviors. Martinez-Garcia & Ferrer (2023) prove that using multiple strategies to communicate works, as they reach audiences that can’t read or write. Journalism, as emphasized by Gálik & Tolnaiová (2022), plays a pivotal role in disseminating accurate information, reducing fear, and mitigating vulnerability during crises.

Maloney et al. (2023) explores how information about disease severity and misinformation is presented within ideological media bubbles, influencing public understanding. The study used a communication model (IHSM–Ideological Health Spirals Model), which was made for politically polarized responses to the Covid-19 threat in the U.S. (Young & Bleakley, 2020). The study text suggests a fresh model for explanation, prompting researchers to consider the interplay between an individual's personal traits and the broader political, media, and societal environment. This interplay influences the likelihood of an individual participating in specific health-related behaviors. The study found that in the case of Covid-19, people had different perceptions about the virus depending on which news they were exposed to, as the news contained different information. Maloney et al., (2023) make the argument that the claim: "Covid-19 is a hoax" was the most common piece of misinformation travelling through news stations. This claim was refuted 100% of the time on CNN, but only a little over half of the time on MSNBC. The study goes on to conclude that the misinformation was brought up a significant number of times on air, with the sole purpose of correcting the misinformation. Maloney et al. (2023) go on to question whether it is a good option to include the misinformation again on air just to correct it, debating whether it would create false memories to individuals watching or not.

Overall, health communication is found to be a highly susceptible arena for online misinformation particularly during the Covid-19 pandemic. The global erosion of trust in health information sources (including governments and media) and the interplay between personal traits and ideological media bubbles is explored, questioning the effectiveness of correcting misinformation on air and the communication strategies during times of a crisis.

4.7 Political Dynamis & Communication

10 articles' key terms pointed them to the group of Political Dynamics and Communication. The rapidly evolving media landscape, characterized by a fusion of traditional and digital channels, has raised critical questions about the impact of misinformation on political dynamics and public engagement. Although numerous studies have examined the impact of a combined system of information channels on political involvement and election campaigns, there is limited understanding regarding how the presence of a hybrid media environment exposes individuals to false or misleading information during an election period (Neyazi et al. 2022).

Neyazi et al. (2022) shed light on the vulnerabilities associated with the hybrid media environment, highlighting that while Facebook and Twitter have made strides in countering false information, WhatsApp and Instagram remain susceptible to exposure to false information. The study was based on political misinformation on the U.S. presidential elections in 2016. Molina (2023) discusses more in depth about the impact of disinformation to political interest, stating that the participants in another study showed reduced interest in politics after learning how present disinformation is in the media environment. Furthermore, the study perceived that there are individuals who deliberately share disinformation seen on social media, just because they might agree with the story or the message, and thus intentionally identifying with a political group. Bauer & Clemm von Hohenberg (2021) conclude that people on the internet are not only passive news receivers, but also sharers of the news. In addition, stating that people do become vulnerable to disinformation through different reasons, identifying the following three: people who have low trust in mainstream media, those who lean towards populist right-wing politics and those with lower political knowledge. Rhodes (2021) underscores the insidious role of algorithmic filter bubbles and echo chambers in shaping political ideologies and information consumption patterns. The study reveals partisan variations in responses to the disruption of filter bubbles, highlighting the complexity of addressing vulnerabilities when political affiliations intertwine with information consumption.

Koc-Michalska (2023) investigated the impact of digital media on political campaigns and communication, calling for democracy-oriented government regulations which would enable transparency among political parties and media companies. Freedman (2018) adds to this topic of media policy failures that contribute to circulation of misinformation on social media. The lack of regulation has allowed digital intermediaries to spread misinformation, undermine democratic politics and attack mainstream media. The article underlines the dire need for policies about breaking media monopolies, holding power accountable and using algorithms to public interest. In the digital age, where information is power, understanding and mitigating these vulnerabilities are paramount. The complex challenges they present demand collaborative efforts from researchers, policymakers, and digital platforms to safeguard the integrity of digital communication and foster a well-informed and resilient society.

In a study by Farkas (2023), fake news emerged as a significant political concern in shaping public perceptions of media institutions, highlighting the growing importance of news media as a social institution, particularly during elections. The research also delves into how journalists can inadvertently create gaps in public perception and affect the resolution of political issues. Similarly, the work of Splendore & Curini (2020) sheds light on the increasing visibility of journalists' political leanings, which has a direct impact on the public's trust in traditional media. The study underscores the influence of ideological proximity, an aspect often overlooked in media trust research. In addition, a study by Graziano & Percoco (2017) talks about the role of media in shaping individual attitudes and political decisions. The study suggests that media exposure influences voters' perceptions, particularly among swing voters, (individuals who are not firmly aligned with any particular political party or candidate), and that crime news plays a significant role in influencing their voting choices. The results indicate that TV can affect voters' perceptions through specific channels, particularly by increasing the salience of certain issues like crime, leading to support for specific political parties or coalitions. Similar results were found in another study, where individuals were exposed to opposing political views multiple times on social media, which ultimately led to disconfirmation bias. Disconfirmation bias is the term used to describe the situation when an individual holds a strong belief to the extent that they struggle to acknowledge or accept any evidence or information that contradicts that belief (Study.com, 2023). Furthermore, journalists who use right-wing politicians' Twitter posts frequently to catch the public eye in social media, are inadvertently fueling resentment among left-wing voters against right-wing public personas (Heiss, 2019).

Addressing vulnerabilities and ensuring the integrity of digital political communication demand collaborative efforts from researchers, policymakers, and digital platforms. As information continues to shape political narratives and public discourse, safeguarding the integrity of the media environment remains paramount in fostering a well-informed and resilient society. The essential variable highlighted in these articles is the source of political communication, distinguishing between grassroots citizens and institutional entities. Additionally, studies found people deliberately sharing misinformation aligning with their political views and vulnerabilities were established in people with low media trust, populist right-wing leanings, and lower political knowledge.

4.8 Addressing Vulnerabilities and Building Resilience

8 articles' key terms pointed them to the category of Addressing Vulnerabilities and Building Resilience. What comes to resilience building information, a study by Mensah et al. (2023) found that government information transparency positively influences information quality, credibility, information usefulness and importantly, publics' adoption of Covid-19 pandemic related information. More recently discussed topic has been the inoculation theory, that is used to counter disinformation, specifically astroturf attacks –a tactic used for political and corporate gain in the form of disinformation– regarding social issues, such as Covid-19 and climate change (Boman, 2023). The study by Li & Shin (2023) enhances the discussion on addressing vulnerabilities and building resilience by highlighting the influence of misinformation about e-cigarettes on social media. It underscores the importance of correcting misinformation through credible sources and tailored communication strategies to build resilience against health misinformation. This research aligns with the broader theme of inoculation theory by suggesting that accurate, credible information can act as a preventative measure against misinformation, reinforcing public resilience to health-related disinformation campaigns on social media platforms.

Moussa et al. (2022) found that the preparedness and skills for resilience vary among young individuals, influenced by personal characteristics, social background, and the extent of exposure to essential skills in an educational setting. Digital and news literacy also play a role in resilience, but awareness of misinformation is often a result of wariness rather than critical thinking. In addition to the recipient variable factors, also the sender of the message and the message itself add on to the resiliency or susceptibility that a person experiences (Rainear & Lachlan, 2022).

Furthermore, a study by Stubenvoll et al. (2021) found that individuals with lower political knowledge may come across political content but might lack the political skills needed to navigate through and evaluate its credibility. Recent research supports this idea, showing that individuals with high political knowledge are more adept at distinguishing between quality news and "fake news", as well as differentiating opinions from facts (Mitchell et al., 2018; Van Duyn & Collier, 2019). However, Taber and Lodge (2006) argue that highly knowledgeable individuals are also better equipped to defend their existing worldviews. Consequently, it is unclear whether individuals with high political awareness excel in identifying actual inaccurate information or if they are more prone to categorizing posts from their weak social connections on social media as "fake".

Study by Tsfati et al. (2020) argue that certain audiences may be prone to retaining misinformation labelled as 'fake news', particularly if they experience strategic memory impairments or information overload. It is challenging to make predictions about individuals heavily reliant on mainstream news media. While repeated exposure to fake news enhances familiarity and retention of incorrect information, such audiences are also exposed to corrections and detailed explanations, making them less susceptible to disinformation.

The research by Shufan et al. (2022) on Intel SGX vulnerabilities adds a crucial perspective to the conversation on resilience in cybersecurity. It underlines the necessity of robust security measures and the development of countermeasures to safeguard against sophisticated cyber threats. This study not only identifies existing vulnerabilities but also proposes a framework for enhancing security protocols, thereby contributing to the foundational efforts in building digital resilience against evolving cyber-attacks.

Overall, resilience varies among individuals based on personal characteristics, social background, and exposure to essential skills. Digital and news literacy, along with awareness of misinformation, contribute to resilience while certain audiences may retain misinformation due to memory impairments or information overload.

4.9 Country-Specific Studies

7 articles’ key terms pointed them to the category of Country-Specific Studies. As the group name suggests, these articles studied the phenomena in the context of specific countries. Global media systems and their impact on society is a multi-faceted domain, which is shaped by local cultures, political structures, and technological advancements. In the West Nordic countries, namely the Faroe Islands, Greenland, and Iceland, the media systems, although aligning with the Nordic model in their perception of media as cultural institutions and the centrality of

public service media, face unique challenges. As Ravn-Højgaard et al. (2021) illustrate, these small, democratic welfare states contend with vulnerabilities due to their micro-size. These systems are susceptible to clientelism, and journalists may engage in self-censorship, influenced by both size and distinctive local factors.

The United Arab Emirates presents a different scenario. Moussa, Radwan, and Zaid (2022) explore the resilience of UAE youth to COVID-19 misinformation. Their study reveals a complex interplay between individual agency, digital news literacy, and a top-down approach to misinformation. This underscores the nuanced ways in which young people in non-Western, paternalistic societies navigate the information landscape, especially in the face of a global pandemic.

In the Czech Republic, a post-transition democracy, the media landscape has been significantly impacted by the rise of digital platforms and right-wing populism. Štětka, Mazák, and Vochocová (2021) focus on the disinformation ecosystem, highlighting the challenges posed by online disinformation, automated propaganda, and the consumption patterns of disinformation news websites. This scenario presents a critical examination of the democratic public sphere and the processes of democratic deconsolidation and rising illiberalism.

In Italy, the persuasive power of the media and its influence on political perceptions and voting behavior is evident in the study by Graziano and Percoco (2017). Focusing on the Italian 2001 general election, they demonstrate how media-induced agenda setting, particularly regarding crime, shaped voter attitudes and decisions. This highlights the media's significant role in framing public issues and influencing the political landscape.

In transitional democracies like Ukraine, the boundary work of defining legitimate journalism is crucial, as shown by Yanchenko et al. (2023). The sanctions against Russia-affiliated TV channels and the ensuing public debate underscore the tension between journalistic legitimacy and national security. This case study offers insight into the discourses surrounding legitimate and antagonistic media actors in a politically volatile environment.

From a Ghanaian perspective, Mensah et al. (2023) emphasize the role of government transparency in the adoption of COVID-19 pandemic information on social media. The study suggests that information quality, credibility, and usefulness are crucial in public reception, and government transparency significantly moderates these factors.

Lastly, the Spanish media landscape, as investigated by Masip, Suau, and Ruiz-Caballero (2020), illustrates the dynamics of news consumption in the age of social media. Their findings indicate a shift from traditional selective exposure to a more diverse exposure, facilitated by social networks, suggesting a potential moderation of the echo chamber effect in online news consumption.

These studies collectively paint a picture of the diverse and complex nature of media systems and information dissemination across different global contexts. They highlight the importance of understanding local and cultural specifics, the evolving role of digital platforms, and the intricate relationship between media, politics, and public perception. This chapter underscores the multifaceted nature of media systems and their profound impact on societies worldwide.

4.10 Information Management & Security

7 articles' key terms pointed them to the category of Information Management and Security. A study by Katerynych (2022) provides a critical examination of information security in the context of the ongoing conflict between Ukraine and Russia, with implications for neighboring countries like Poland. The study characterizes a country's information security as a multifaceted security system aimed at safeguarding the nation in the digital realm. This involves overseeing internal state information and effectively protecting national interests in the global information sphere (Internal and External Situation…, 2014. Mentioned in Katerynych, 2022, 38). An information security threat in this context encompasses a multitude of deliberate actions, both domestic and foreign, that exploit vulnerabilities within a nation's information environment. These actions aim to undermine its security, stability, and reputation, necessitating the development of comprehensive strategies and policies to effectively mitigate such multifaceted threats. This challenge arises from the inherent difficulty in devising effective strategies to combat various forms of threats and counter attacks within the realm of information and communication. Within this context, it is notable that there is a perceived shortfall in Ukraine's information security system's capability to identify, analyze, and decisively counter threats to national security stemming from the information domain. (Katerynych, 2022.) Much like Katerynych (2022) highlights the complexity of safeguarding a nation's digital space, Shufan (2022) draws attention to the intricate challenges of securing technology against sophisticated attacks. Both pieces of research stress the necessity for multi-layered security strategies that encompass policy formulation, technological innovation, and increased awareness to protect against threats to information integrity and security, reflecting a unified approach in addressing vulnerabilities across different realms of the digital and geopolitical landscape.

Furthermore, Katerynych's (2022) analysis suggests that Polish journalists and editors might not be well-informed about information security principles outlined in the National Security Strategy. Even though most of the respondents are aware of the threats regarding information space and believe it is critical to regularly update the state documents regarding information security, both Polish and Ukrainian journalists rarely refer to the information security provisions during their work. This suggests a possible lack of authority of these provisions in both countries and thus indicating an insufficiently developed information policy in these nations (Katerynych, 2022). Many Polish participants believe that the media owner's role impacts how journalists and editors perceive and adhere to state information security principles. The article underscores the crucial role of journalists in defending information integrity during times of conflict. Findings from this study reveal that journalists in both Ukraine and Poland perceive existing information security measures as inadequate. This highlights the importance of journalists playing a role in influencing information policies, a topic also addressed in chapter 4.1.1, Journalists Responsibilities. According to Media Pluralism Monitor (MPM), the absence of media ownership transparency creates challenges for the public in recognizing potential biases in media content, undermines editorial independence, and represents the most vulnerable facet of media systems, susceptible to both commercial and political influences (Baptista, 2022).

Heiss, von Sikorski and Matthes (2022) focus on information disclosure, making the notion that transparency is mainly seen as a means to foster accountability, forming a central aspect of ethical journalistic codes. The Society of Professional Journalists' Code of Ethics (2014) defines transparency as "clarifying one's decisions to the public." Long-standing ethical principles include transparency in sourcing and the responsibility to reveal conflicts of interest, such as political affiliations and potential bias. The concept that providing extra reporting material enhances credibility is a more recent response to the growing perception of a politically polarized media environment.

Baptista (2022), suggests establishing an independent public agency to encompass licensing, handling complaints and sanctions, rulemaking, mandatory consultation for management board appointments in public service media, and monitoring programming. Portugal has founded such in 2016; Portuguese Media Regulatory Authority (ERC). The primary objectives of the ERC revolve around ensuring two key principles: pluralism and diversity. ERC's regulatory council, comprising five members elected by Parliament, holds significant powers within the EU regulatory framework. ERC is dedicated to safeguarding pluralism and diversity, remaining vigilant against attempts by political and economic entities to compromise media independence. The regulator has, on multiple occasions, taken actions aligned with this vision, preventing acquisitions and mergers that could undermine cross-media concentration and impact other aspects of pluralism, such as the political independence of news outlets and the editorial autonomy of journalists (Baptista, 2022).

Zalmanson et al. (2022) pivot into websites and their security measures. Websites with social cues, such as liking or rating content indirectly increase users' willingness to disclose private information (e.g., full name, address and birthdate) by enhancing users' perceptions of the website as a social environment. Furthermore, the results of the study indicate that policymakers should focus on preventing websites from incorporating deceptive or untrustworthy indicators of trust. Zalmanson, Oestreicher-Singer & Ecker (2022) argue that implementing third-party trust signals that are challenging to counterfeit, such as security certificates with encryption capabilities granted by external authorities. However, the effectiveness of such a policy relies on users having a solid understanding of information security and the ability to distinguish reliable from deceptive trust signals. To promote this knowledge, many prominent technology companies, such as Microsoft, Apple, and Google, known for their widely used web browsers, have incorporated user-friendly warnings and pop-ups to help users recognize when a website may pose risks to their personal information and computer security (Zalmanson, Oestreicher-Singer & Ecker, 2022). Moreover, it may be advantageous for web browsers to provide similar alerts for websites that display deceptive trust cues. For instance, a website claiming to be safe and trustworthy but failing to adhere to privacy policies or use encrypted data delivery. By doing so, users exposed to social cues can exercise greater caution and refrain from sharing information that could compromise their privacy and safety (Zalmanson et al., 2022). Hwang and Jeong (2023) explore the role of information seeking and processing in the exposure to and acceptance of misinformation, particularly in the context of COVID-19 in South Korea. The findings suggest that information avoidance, rather than information seeking, predicts misinformation exposure. Additionally, heuristic processing amplifies the acceptance of misinformation upon exposure. These results emphasize the importance of understanding information processing behaviors to mitigate misinformation's impact, highlighting a crucial intersection with information management and security strategies to combat misinformation effectively.

The central theme across these articles is the distinction between authorized and unauthorized aspects of information management and security. This encompasses a range of issues, from national security and journalistic ethics to individual privacy and online trustworthiness. Moreover, information policies effect on pluralism and diversity of social media platforms are found to increase or decrease disinformation resiliency. Studies emphasize the importance of understanding information processing behaviors in combating misinformation.

4.11 Understanding Information Polarization

7 articles' key terms pointed them to the category of Understanding Information Polarization. While there are several reasons for information polarization, Sanchez and Baselga (2023) argue that online media platforms create polarization by enabling echo chambers. Thus, the chapter is divided into a subcategory *'Algorithmic Bias, Filter Bubbles and Echo Chambers'*. Moreover, the authors argue that polarized media landscape creates further difficulties in reaching rational, widely accepted conclusions on any topic. The media play a crucial role in determining the extent of disinformation in society, exerting significant influence (Sanchez and Baselga, 2023). The functioning of journalists and news reporters involves, to some extent, the use of inductive reasoning. The effectiveness of the democratic system relies on their efforts to create a common ground for debating issues and reaching consensus. The media is perceived as a channel for information flow, aiming to establish well-reasoned and widely shared opinions (Sanchez and Baselga, 2023). Nevertheless, challenges persist in the form of a lack of consensus and the polarization of public opinion, even on scientifically grounded topics like climate change, posing significant issues for society (Sanchez and Baselga, 2023). This predicament cannot be solely attributed to the motives of

certain entities manipulating information; it is also largely a result of our inherent cognitive inclination to perceive matters with bias. Any communication model must consider this factor to determine how the media can best contribute to mitigating these effects. Nevertheless, while the media can worsen the issue, they are not its root cause (Sanchez and Baselga, 2023).

When it comes to political information, whether it's accurate or not, the filtering process within filter bubbles (see chapter 4.11.1) and its reinforcement in echo chambers results in the creation of homogenous information streams. Prior research has revealed that people tend to become divided and polarized when they are continually exposed to unchallenged political content (Levendusky, 2013). Furthermore, Levendusky (2013) demonstrates that when individuals watch media that aligns with their existing beliefs, they become more extreme in their views, and these effects persist for several days. Rhodes (2021) investigated how disinformation can slip through people's conscious screening when it’s mixed with content, they find agreeable, concluding that it is indeed the case. Stubenvoll et al. (2021) investigated perceived misinformation exposure and its consequences, finding that perceived misinformation exposure (PME) leads to further polarization among some individuals. In addition to algorithmic biases, people consciously choose individuals in their network who share the same point of view and preferences, thus avoiding political (or any kind of) information that contradicts their existing views.

A study by Masip et al. (2020) investigated if social media use increases the exposure of Spanish citizens to non-like-minded news. The results are contradictory, although people (60.9% of the study population) access non-like-minded media sometimes, only 27% of the study population did it frequently. Thus, confirming that using social media exposes individuals to different ideologies online, broadening their own views with these platforms by following different minded people, or so called devil’s advocates. However, this does not mean that the individuals online are not vulnerable to disinformation, but it does seem to work as a way to build resilience in an online setting. Furthermore, Masip et al. (2020) found evidence that the recent findings on echo chambers and filter bubbles do not apply in the Spanish context, as the majority of Spanish people are not active in online spaces that align with specific ideologies. However, this again does not mean that even though the people don’t consciously seek information from online communities that share an ideological affinity, that they would not be exposed to, or affected by them unconsciously. (Masip et al. 2020.)

In the context of understanding information polarization, the key aspect illuminated by four articles in this chapter is the differentiation between technological and psychological polarization. It’s found that the media's role in information polarization, exacerbated by echo chambers and filter bubbles contribute significantly to misinformation susceptibility. Also, contradictory results are found on social media's impact, suggesting that exposure to diverse views can build resilience.

4.11.1 Algorithmic Bias, Filter Bubbles & Echo Chambers

The literature looks at filter bubbles, echo chambers and the types of information processing associated with them in order to better understand how people become susceptible to misinformation (Rhodes, 2021). Bartley et al. (2021), Rhodes (2021), Du (2023), Shin (2023), and Liao (2023) explore the realm of vulnerabilities associated with algorithm-based systems, as their articles uncover vulnerabilities that arise from the profound influence of algorithms and biases, necessitating a comprehensive understanding of their implications for the digital age.

One of the primary vulnerabilities that emerge from these studies is the supreme role of algorithms in shaping the digital information ecosystem. Bartley et al. (2021) suggest that preexisting cognitive biases, such as social influence and position bias, when combined with algorithmic suggestions can magnify online trends, resulting in "irrational herding" and distorting how individuals perceive the true value of content. For example, Twitter's algorithms are made for personalization and content selection, which compile a user's timeline based on their friends' tweets, subtly distort and bias the information that users are exposed to (Bartley et al., 2021). The personalized timeline on Twitter is shaped by the curation of popular tweets, and this curation is responsible for the disparity in friend exposure within the personalized timeline. Ultimately some accounts seen on the feed are disproportionately favored. Thus, algorithmic suggestions merge with individual choices to transform the information ecosystem, creating an echo chamber (Bartley et al., 2021).

Rhodes (2021) demonstrates how algorithmic filter bubbles and echo chambers exert a potent influence on individuals' exposure to fake news, driven by political affiliations. Echo chambers are personalized communication environments that revolve around users' capacity to follow individuals who share their like-minded beliefs. The algorithmic filter bubbles are designed to expose individuals to agreeable content in order to increase their screen time on a specific platform, which provides significant income for these companies and thus are unlikely to alter these algorithms unless forced by regulations (Mims, 2017). Similarly, Du (2023) unveils the impact of algorithms on news consumers, particularly within AI-powered news apps. Shin (2023) introduces the concept of Accuracy Alerts, highlighting the capacity of algorithms to mitigate misinformation on social media. Liao (2023) delves into users' perceptions of various algorithmic-based news recommender systems, elucidating their preferences influenced by algorithmic recommendations. These findings collectively underscore the central role of algorithms in curating, tailoring, and influencing the information individuals encounter in the digital sphere. For example, automation bias, particularly within recommendation algorithms, reflects individuals' tendency to follow computer-generated suggestions without actively seeking contradictory information (Cummings, 2004). This bias is heightened during information overload, a prevalent issue in today's online news landscape (Parasuraman & Manzey, 2010). This vulnerability exposes individuals to potential influence, as they may accept algorithmic recommendations without critically assessing alternative sources of information.

A critical vulnerability illuminated by Rhodes (2021) and Du (2023) pertains to filter bubbles and echo chambers. These studies reveal that individuals exposed to information aligned with their preexisting beliefs are more prone to accepting fake news, a vulnerability exacerbated within filter bubbles. Du's (2023) work reinforces this by exposing users of AI-powered news apps to potential biases and concerns regarding the omission of diverse perspectives. The risk of individuals becoming confined within information environments that reinforce their existing biases poses a formidable challenge, as it hampers the development of well-rounded perspectives, fosters polarization, and hinders critical thinking. This vulnerability underscores the necessity of addressing filter bubbles and echo chambers to preserve an informed and open digital communication landscape. Shin's (2023) research introduces the vulnerability of combating misinformation with Accuracy Alerts. While effective, this mechanism reveals the challenge of countering misinformation propagated by algorithmic news sources. Algorithms are instrumental in the dissemination of false information, and mitigating their impact represents a significant vulnerability that demands attention in digital communication. Liao's (2023) study contributes by uncovering a preference for collaborative filtering systems among users, a preference influenced by the homophily heuristic. This underscores the vulnerability of users' trust in algorithms, as they tend to rely on recommendations from sources or individuals similar to themselves. This trust dynamic can lead to insular information consumption, further accentuating the challenges associated with filter bubbles and echo chambers.

In sum, the vulnerabilities stemming from the articles authored by Rhodes (2021), Du (2023), Shin (2023), and Liao (2023) necessitate a holistic approach to address the profound impact of algorithms and biases within the digital communication landscape. These vulnerabilities include algorithmic dominance, the peril of filter bubbles and echo chambers, the challenge of combating algorithm-driven misinformation, and users' susceptibility to trusting algorithms that align with their existing beliefs. As the digital communication landscape evolves, understanding and mitigating these vulnerabilities becomes paramount to ensure an inclusive, diverse, and trustworthy information environment conducive to democratic discourse and critical thinking.

4.12 Cybersecurity and Technology

4 articles’ key terms pointed them to the category of Cybersecurity and Technology. Nicoli et al. (2022) present a compelling exploration of blockchain technology's potential to address critical issues within the information and communication sector. Their examination centers on the capacity of blockchain to mitigate the democratic deficit and combat challenges such as post-truth politics and populism that afflict the contemporary information landscape. Blockchain technology, characterized by its decentralized, transparent, and traceable nature,

emerges as a promising solution to the multifaceted challenges faced by the information and communication sector. It offers the prospect of enhancing content security, tracing the origins of news sources, and empowering users to authenticate the authenticity of information. Moreover, the advent of blockchain-based social and news media platforms holds the promise of curtailing misinformation and censorship while championing decentralization and user control. However, this optimism is tempered by the acknowledgment of several vulnerabilities and challenges associated with blockchain integration. Slow transaction speeds, energy consumption concerns, and socio-economic and political implications loom as potential obstacles to the seamless adoption of blockchain technology. These vulnerabilities underscore the need for careful consideration and mitigation strategies in harnessing blockchain's transformative potential.

At its core, the central question posed in this article revolves around blockchain's role in mitigating the democratic deficit and restoring trust in the information ecosystem. It highlights the transformative power of blockchain technology, not merely as a technical innovation but as a catalyst for fostering a healthier democratic discourse. By instilling trust in information sources and enabling greater transparency, blockchain has the potential to reshape the dynamics of information dissemination. What sets this article apart is its distinct focus on technological solutions to address misinformation and its broader impact. It emphasizes the necessity of a comprehensive approach that encompasses systemic changes beyond technology alone to fully address the profound challenges confronting the contemporary information landscape.

According to Qahri-Saremi & Turel (2023), for users and platform managers alike, a comprehensive understanding of the intertwined factors, encompassing likability, ostracism, and FOMO, can serve as a strategic tool in mitigating phishing risks. Awareness of techniques such as ghosting and breadcrumbing (see chapter 4.4), along with their role in creating potent situations that tempt users into engaging with phishing attacks, empowers individuals to remain vigilant and alert to potential threats, thereby reducing Click-Through Rates (CTR) and enhancing overall cybersecurity measures (Qahri-Saremi & Turel, 2023). In addition, interventions are introduced later on in the study, making a case for warning or fear appeal messages in friend requests on social media. If received from individuals who lack mutual connections with the user, have a history of sending friend requests to multiple users on the platform, or have been identified or reported by other users, the warning messages could reduce phishing susceptibility (Qahri-Saremi, 2023).

Another study by Chatterjee et al., (2023) focuses on the role of fake news and misinformation in supply chain disruption and how it can be moderated through technology. The significance of industry 4.0 is seen as pivotal in addressing the spread of misinformation and fake news, which poses disruptions to supply chains (Endsley, 2018). The emerging technologies include IOT, cloud computing and AI machine learning. They enable the exploration of the origins, dissemination patterns, and specific content of misinformation or fake news, offering the potential to address its spread and effectively handle it amid disruptions in the supply chain (Jayawickrama et al., 2019; Olan et al., 2016).

According to Chatterjee et al., (2023) using these technologies is prevalent in building resilience against misinformation online and identifying the authenticity of online information. However, it's noteworthy to mention that specific software is not named, leaving some speculation on how they can be used. Moreover, organizations should have standard operating procedures ready to be implemented whenever needed during an information crisis, where misinformation or disinformation has spread. Thus, the employees of the firm would know how to act and take a skeptical stance on information provided through social media (Chatterjee et al., 2023). Afterall, 42% of false news stories are accessed through social media, whereas actual news sites are only accessed 10% of the time (Endsley, 2018).

The central theme is discerning whether cybersecurity and technological challenges are internally or externally caused. This encompasses a range of issues, from the adoption and implications of blockchain technology to the psychological factors influencing susceptibility to cyber threats and the role of advanced technologies in mitigating the spread of misinformation and its impacts. Blockchain's role in mitigating the democratic deficit and restoring trust in the information ecosystem could be significant and the literature emphasizes the need for a comprehensive approach beyond technology.

4.13 Articles with no Keywords

2 articles of the literature review had no key terms to be found. The article by Matt Law (2023) contributes to the discussion on digital communication vulnerabilities by underscoring the importance of Crisis and Emergency Risk Communication (CERC) in mitigating misinformation during health crises. It highlights how Occupational Safety and Health (OSH) professionals can leverage evidence-based communication strategies to combat misinformation, which is a significant vulnerability in digital communication, especially during emergencies. The focus on preparation, execution of CERC strategies, and addressing misinformation directly tackles key aspects of digital communication vulnerabilities, emphasizing the need for credible, timely, and transparent information dissemination.

The article by Pyrhönen and Bauvois (2019) examines how conspiracy theories like Macronleaks, Pizzagate, and Voter Fraud infiltrate the political news cycle, highlighting vulnerabilities within digital communication. It focuses on "produsers" who blend roles of producers and users in disseminating conspiracy narratives across both mainstream and "counter media" platforms. This exploration into the "reinformative toolkit" used by these produsers emphasizes the challenges in distinguishing between legitimate news and conspiracy-driven content, underlining the complexities and vulnerabilities present in the hybrid media system. Such dynamics facilitate the spread of disinformation, impacting public discourse and trust in media institutions. Given the article's focus on events like Macronleaks and Voter Fraud, the article ties closely to political communication and how it's influenced by digital media

5 CONDUCTING THE FRAMEWORK

To address the research questions posed in this thesis, a framework was developed to identify vulnerabilities of digital communication efficiently. The following chapters offer a more in-depth analysis of the articles included in the systematic literature review, augmented by further supporting research, to yield thorough and comprehensive conclusions. This supplementary research encompasses both scholars mentioned at the thesis outset and new studies discovered through insights acquired from the literature review.

5.1 Level of Analysis

In the examination of the systematic literature reviews articles, one objective became to discern the scope from which each article approached the concept of vulnerability. Bjola and Papadakis (2020, p. 641) proposed a method that separates the analysis of disinformation experiences into two levels: one focusing on individual or collective experiences (microsphere), and the other on the impact of disinformation on diplomatic policy decisions (macrosphere). This approach aims to create a systematic and coherent way of categorizing disinformation experiences. However, this study took the liberty of adding a third dimension, meso-level into account. Building on this, the study employed a three-tiered analytical approach spanning from broader to more specific levels: macro, meso, and micro. This distribution is supported not only by the systematic literature review, but also by Pamment (2018) and Hansson et al.'s (2020) levels of vulnerabilities: Individual and Cognitive Vulnerability; Social-Structural and Public Opinion Vulnerability.

It is important to acknowledge that the levels are interconnected, with the meso level exerting influence over the micro level, and the macro-level exercising authority over the meso level. When there is an issue at the macro level, it has a consequential impact on individuals at the micro level. However, issues originating at the micro level may not always be immediately evident when considering the macro level. These levels solely offer a perspective through which vulnerabilities are analyzed.

5.1.1 Macro

At the macro level, an analysis is conducted to explore vulnerability within a broader context, encompassing societal, national, and global dimensions. The rampant spread of fake news and misinformation has morphed into a worldwide predicament, exerting extensive influences on societies, electoral processes, and global public perceptions.

This global phenomenon finds a vivid illustration in Russia's actions in Ukraine, which have exposed vulnerabilities in international and national digital communication. This is well-documented in Katerynych's (2022) study on information security in Ukraine and Poland, where both nations grapple with an array of information-related threats, further compounded by the ongoing military conflict in Ukraine and a migrant crisis at the Polish border. Additionally, the news media depicts fake news, mainly viewing it as a major threat to national security (Farkas, 2023). Likewise, global issues of misinformation and disinformation have been thrust into the spotlight by the COVID-19 pandemic. The worldwide landscape of COVID-19 misinformation is thoroughly examined, revealing vulnerabilities that transcend national boundaries and emphasizing the need for multifaceted solutions. Trust emerges as a recurrent theme that transcends borders. The amplification of political crises during the pandemic due to distrust in institutions becomes evident (Martínez-García & Ferrer, 2023). Furthermore, the disparity between trust in government and media and the perception of COVID-19 misinformation is a focal point (Moussa et al., 2022). Inadequate crisis communication contributes to the erosion of trust and poses challenges to the resilience of society (MacKay et al., 2023).

5.1.2 Micro

Similarly, at the micro level, an in-depth analysis unveils vulnerabilities within individual and small group dynamics, shedding light on the intricate challenges associated with trust, information authenticity, cognitive susceptibility, educational disparities, echo chambers, and political ideologies.

For instance, trust, a fundamental element in information sharing, is a micro-level vulnerability that profoundly influences how individuals assess the credibility of their information sources. Media trust is often influenced by an individual's limited political knowledge, rendering it sensitive to political factors (Stubenvoll, 2021). In a digitally dominated era trust in institutions has undergone a transformation, making it increasingly intricate for individuals to discern reliable sources amidst an overwhelming influx of information. This vulnerability is particularly apparent when the sheer volume of information makes it challenging to differentiate credible sources from deceptive ones. (Koc-

Michalska, 2023.) Conversely information source integrity shapes individual trust and beliefs. Blurring the lines between trustworthy and untrustworthy sources complicates this vulnerability, especially when individuals are drawn to information that aligns with their preexisting beliefs. (Bauer & Clemm von Hohenberg, 2021.) The micro-level analysis of digital communication vulnerabilities reveals a complex interplay between cognitive limitations, strategies to counteract disinformation, and the dynamics of trust.

5.1.3 Meso

Situated between the two extremes, the meso level focuses on scrutinizing vulnerability within the framework of organizations, communities, or institutions. At the meso level, the focus shifts to how organizations navigate the complexities of digital communication vulnerabilities.

Media institutions and journalists have a significant impact on public trust, particularly in times of crisis. Media platforms, as organizational structures, have a pivotal role in molding the digital environment. Consequently, while these organizations are vulnerable themselves, they also contribute to creating a digital landscape that is prone to specific vulnerabilities. (Hameleers et al., 2022; Gálik & Tolnaiová, 2022; Balod & Hameleers, 2021; Marwick & Lewis, n.d.; Baptista, 2022.) When examining the organizational level, digital communication vulnerabilities affect not just external perceptions but also internal organizational dynamics and relationships.

5.1.4 Vulnerability Paths

Given the interconnections among the levels, the meso level wields influence over the micro level, while the macro level holds authority over the meso level. Consequently, issues originating at the macro level have repercussions for individuals at the micro level (E.g., authority health disinformation) and vulnerabilities originating at the micro level may have significant effects on the macro level (E.g., political speeches influenced by subconscious biases). However, effects originating from micro level may not always be immediately apparent, as the contrary event. These levels serve as distinct lenses through which vulnerabilities are assessed. This underscores the need for a method to navigate vulnerabilities across these levels.

The concept of path dependency, as initially introduced by David (1985) and Arthur (1988), provides a valuable framework for analyzing how technology, institutions, and historical developments unfold over time. Path dependency highlights the enduring influence of past choices, leading to distinct historical trajectories that can be challenging to alter, even if those decisions were not the most efficient at the time. In essence, it suggests that decisions made at a particular moment can significantly mold and restrict future choices and outcomes, even when those initial decisions were arbitrary or based on limited information. This concept has since been applied in subsequent research. For example, in Layton and Duffy's (2018) article, they discuss how path dependency plays a vital role in shaping the growth and evolution of marketing systems. In a similar vein, this study delves into the idea of a "vulnerability path," which shares commonalities with the concept of path dependency. In simple terms, an attack or exploitation of a single vulnerability could have far-reaching and substantial consequences. This implies that one vulnerability can profoundly influence and constrain future efforts to enhance resilience, similar to the concept of path dependency.

The concept of a "vulnerability path" was introduced by Pescaroli and Alexander (2016) to comprehend the evolution of vulnerabilities within critical infrastructure, which includes digital communication networks. It suggests that vulnerabilities are not solely the result of natural forces but are influenced by a complex interplay of factors, including social systems, power dynamics, economic models, and cultural constraints. This path of vulnerability development encompasses multiple layers and progresses through interactions among root causes, dynamic pressures, and unsafe conditions. Pescaroli and Alexander (2016) emphasize that these vulnerabilities can emerge at various spatial and temporal scales, including national and international levels. This underscores the idea that vulnerabilities within critical infrastructure are interconnected and can be influenced by political decisions, cultural influences, and organizational weaknesses. This study applies the logic onto digital communication networks. In summary, the "vulnerability path" concept describes the dynamic and multifaceted nature of vulnerabilities in critical infrastructure, highlighting that they evolve over time and are shaped by various factors beyond just physical or natural factors (Pescaroli & Alexander, 2016).

The idea of this study’s "vulnerability path" not only depicts the sequence of events and elements that make individuals, populations, or communities susceptible to harm but also aids in comprehending how a single instance of exploitation can evolve over time. In essence, the vulnerability path progresses from its initial starting point to its ultimate destination, deriving from the actor's (see chapters 5.2.1. & 5.2.1.1) original motivations. The framework presented in this research suggests that identifying the ultimate impact of vulnerability is relatively straightforward. However, once this outcome is pinpointed, it might be possible to retrace the steps along the path to uncover its initial source.

5.2 Framework Elements

Upon reviewing the literature, it was evident that a variety of elements contribute to vulnerabilities in digital communication. These elements are not entirely similar in nature and therefore understanding these vulnerabilities requires a systematic breakdown of these contributing elements into more fundamental components. Wardle's (2017) framework comprises three elements of information disorder: agent, message, and interpreter. Agents play a crucial role in all phases of the information chain, including creation, production, and distribution. They can be official entities like intelligence services or political parties, as well as unofficial groups of citizens. Messages can take various forms, such as in-person communication, text, or audio/visual material. In this study, the focus is specifically on digital communication. Interpreters are influenced by socio-cultural status, political positions, and personal experiences, creating a dynamic where individuals are inclined to accept information aligning with their worldview. This complexity complicates solutions to information disorder, as providing quality information alone may not be sufficient. (Wardle, 2017). The framework conducted in this study utilizes these components as a base work to further examine the construction of digital communication's vulnerabilities.

5.2.1 Actor

Based on Wardle's (2017) agent, **the actor** is essentially the producer behind harmful acts distributed through means of digital communication. Furthermore, the actor can be divided into two: **intentional actor** and **unintentional actor.** This distinction mirrors the differentiation between misinformation and disinformation, where the former is disseminated without harmful intent, while the latter is shared deliberately (Pamment, 2018; Wardle, 2019). The key factor distinguishing these two types of actors is their intent to cause harm. For example, an individual might inadvertently spread misinformation despite having good intentions. In contrast, an intentional actor deliberately seeks to exploit vulnerabilities for political, financial, or social advantage (Wardle, 2019).

5.2.1.1 Attack Vectors

When examining vulnerabilities of digital communication, the boundary between communicational concerns and data security issues is notably delicate, as the literature review highlighted. Therefore, the framework conducted here separates human and non-human vulnerabilities from the attack vector point of view, based on whether the aim is to manipulate human behavior or the deployment of social engineering tactics, or to exploit susceptibilities inherent in software, hardware, or network infrastructure. The realm of digital communication requires to focus not only on the vulnerabilities associated with human behavior but also those related to the communication platforms and environments. The attributes of the vulnerabilities therefore vary along a spectrum extending from human-centric to non-human-centric.

Human factors refer to the manipulation of human behavior or the deployment of social engineering tactics. This includes intentionally influencing the actions or decisions of individuals with the aim of achieving specific objectives. Conversely, the non-human category encompasses the exploitation of susceptibilities inherent in software, hardware, or network infrastructure. This pertains to the strategic utilization of vulnerabilities embedded in technological components and systems. Thus, two separate attack vectors are identified. As the objective of this study is to define vulnerabilities of digital communication over data security, further focus is directed to the human side.

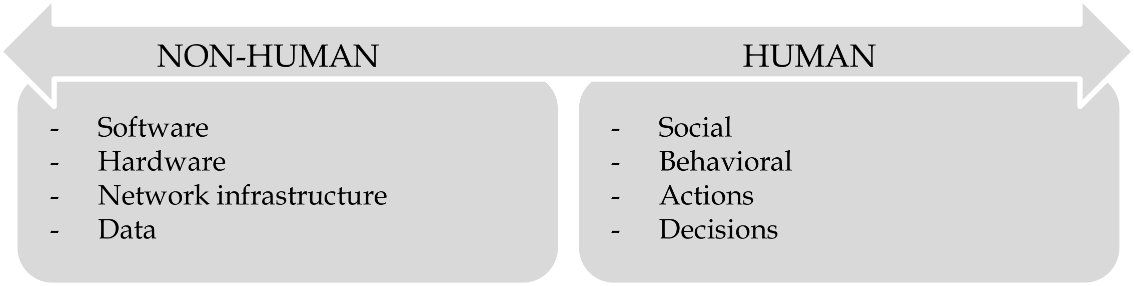


FIGURE 2 Non-Human – Human Continuum

5.2.2 Delivery

Building upon Wardle's (2017) concept of the message, this research expands its scope to encompass the **delivery**, thereby incorporating the message, its distribution channel, and the perceived entity responsible for its dissemination. The literature review highlighted how factors like the formal authority and regulatory framework of the medium influence its perceived trustworthiness or lack thereof (Chadwick, 2022). Additionally, media ownership transparency has proven to contribute to individuals' perspective about their trustworthiness (Craufurd-Smith, Klimkiewicz & Ostling, 2021). For example, according to the Media Pluralism Monitor (MPM), most countries in the European Union reach the minimum level of transparency through the requirement of ownership disclosure to public bodies. However, some countries are not covered by media-specific laws mandating either upward (legal and administrative) or downward (civic) disclosure. Upward transparency renders media actors accountable to regulatory bodies or public administration (for the purposes of auditing and monitoring of media performance and markets). Downward transparency makes the media accountable to civil society, investors and the public (Bernstein, 2017; Edwards and Hulme, 1996; Fox and Haight, 2011; Kolker and Kulldorff, 2013) and facilitates informed financial, personal and political decision-making.
To analyze this, a matrix with two axes was created: one extending from unregulated to regulated channel, and the other from unofficial entity to official entity.

5.2.2.1 Entity Officiality

The continuum of Official Entity – Unofficial Entity differentiates between the sources of information based on their formal recognition and authority. Official entities, such as public servants, law enforcement, and politicians, are formally recognized and operate within established institutional frameworks. Their communications carry the weight of officialdom but can vary in perceived trustworthiness depending on the channel used for dissemination. Unofficial entities include individuals and informal groups that lack formal recognition and institutional backing. Despite their unofficial status, in contexts where institutional trust is low, these entities can gain credibility, especially when they use unregulated channels like social media to communicate (Bauer & Clemm von Hohenberg, 2021; Zimmermann and Kohring, 2020; Bennet & Livingston, 2018; Rhodes, 2021).

As the officiality is based on the authority and formal recognition, the *Unofficial Entity* involves a rather wide range of actors. Regular individuals, despite not having the formal recognition or authority of official entities, can significantly influence public opinion and contribute to the dissemination of information—or misinformation—through personal networks and social media platforms. Conversely, celebrity trust bases on both cognitive and affective dimensions. People trust celebrities who they perceive as competent, responsible, reliable (cognitive dimension), and emotionally resonant (affective dimension). The cognitive dimension involves rational evaluation of the celebrity's trustworthiness and reliability, while the affective dimension involves emotional connections and feelings towards the celebrity. (Hussain et al., 2021). Additionally, strong parasocial relationships between social media influencers and their followers enhance trust. Followers who develop these one-sided relationships with influencers often perceive higher credibility and are more likely to be influenced by their endorsements. (Breves et al., 2021). Celebrities account for a significant portion of the misinformation while attracting disproportionate attention from users. This underscores the double-edged sword of celebrity influence, where trust in their authority can lead to the spread of harmful misinformation if not properly checked. (Gisondi et al., 2022).

5.2.2.2 Channel Regulation

Regulated Channel – Unregulated Channel -continuum focuses on the mediums through which information is disseminated. Regulated channels, such as official websites and mainstream news media, are subject to oversight, ethical standards, and gatekeeping processes that aim to ensure the accuracy and reliability of the information. These mechanisms contribute to making regulated channels generally more trustworthy (Balod & Hameleers, 2021; Tandoc et al., 2012; Chadwick, 2022). Unregulated channels, notably social media platforms, lack such formal oversight and are characterized by the rapid dissemination of information without the same level of scrutiny or responsibility. The nature of these channels can affect the perceived reliability of the information shared, regardless of the entity's official or unofficial status.

5.2.2.3 Distribution Credibility

Four sections are formed: Unregulated Channel, Official Entity; Unregulated Channel, Unofficial Entity; Regulated Channel, Unofficial Entity; and Regulated Channel, Official Entity. It's important to note that no specific quadrant in this matrix can be definitively labelled as trustworthy or untrustworthy, as the perception of trust is subjective and varies among different audiences (Krause, 2022). The matrix's quadrants interact with the audience types: how they perceive and interpret the message's delivery, shaped by the officiality of the entity communication and the regulation of the chosen channel.

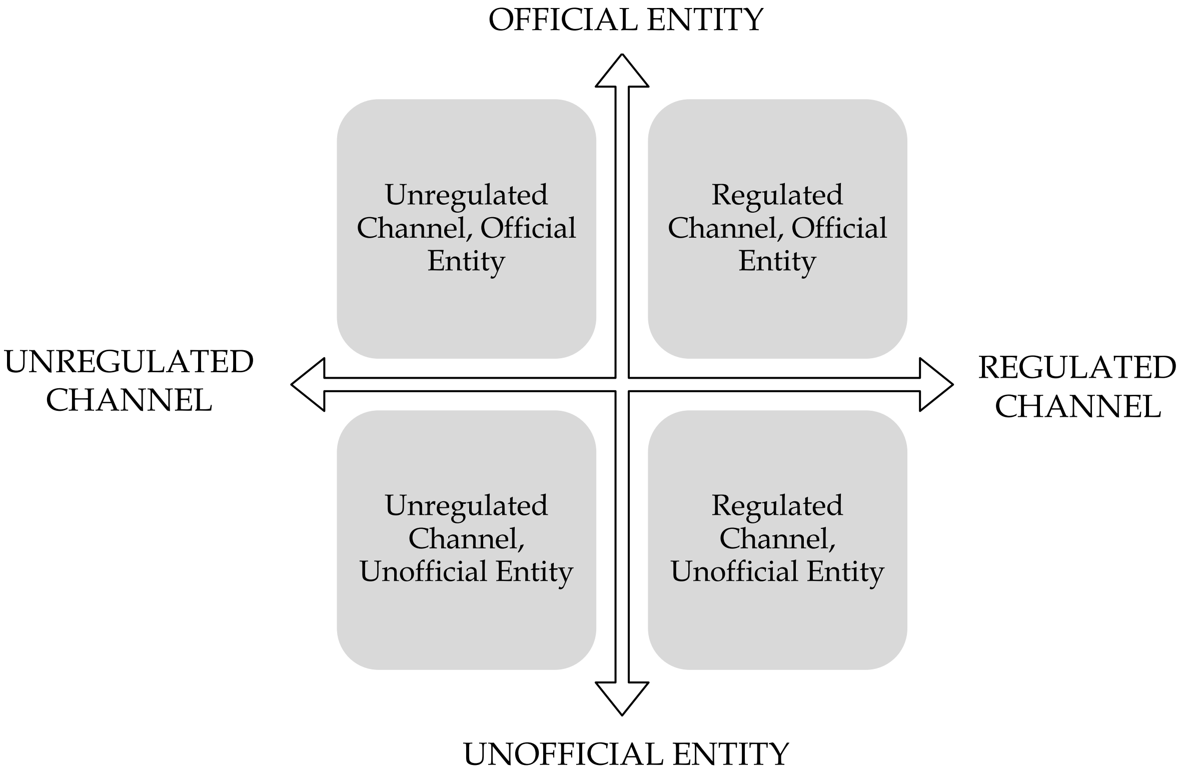

OFFICIAL ENTITY
Unregulated Channel, Official Entity
Regulated Channel, Official Entity
UNREGULATED CHANNEL
REGULATED CHANNEL
Unregulated Channel, Unofficial Entity
Regulated Channel, Unofficial Entity
UNOFFICIAL ENTITY

FIGURE 3 Distribution Credibility

TABLE 11 Distribution Credibility variable

Arena	Description	Attributes
Unregulated Channel, Official Entity	Formal entities use unregulated platforms (e.g., social media) for information dissemination.	Increased accessibility and direct audience engagement, potential credibility issues due to lack of traditional oversight.
Regulated Channel, Official Entity	Official entities communicate through regulated channels, enhancing message validity.	High credibility and trust, though effectiveness may be influenced by general institutional trust levels.
Unregulated Channel, Unofficial Entity	Informal actors engage through similar unregulated channels, lacking formal oversight.	Flexibility, potential for rapid dissemination, credibility varies with audience perception and context.
Regulated Channel, Unofficial Entity	Non-official entities using regulated mediums like mainstream media or official websites.	Subject to gatekeeping and ethical standards, potentially more trustworthy despite the communicator's unofficial status.

The "*Unregulated Channel, Official Entity*" category encapsulates formally recognized entities such as public servants, law enforcement or politicians utilizing unregulated mediums, notably social media platforms, for disseminating information. These mediums often represent newer technologies or are not governed by traditional regulatory frameworks.

Conversely, the "*Unregulated Channel, Unofficial Entity*" group comprises non-institutional entities, including individuals or informal groups, engaging with similar unregulated channels. The absence of formal oversight in these channels and actors might influence the perceived reliability of their communications. However, in scenarios where institutional trust is eroded, these informal communications via social media may gain relative credibility (Bauer & Clemm von Hohenberg, 2021; Zimmermann and Kohring, 2020; Bennet & Livingston, 2018; Rhodes, 2021).

The "*Regulated Channel, Unofficial Entity*" segment involves non-official entities leveraging regulated mediums like official websites and mainstream news media. The regulated nature of the channel does not necessarily enhance the perceived authenticity of the message due to the unofficial status of the communicator (Bearth & Siegrist, 2022). However, the traditional channels have gatekeeping, limitations and ethical responsibilities to stand up to, making them more trustworthy (Balod & Hameleers, 2021; Tandoc et al., 2012; Chadwick, 2022). In addition, the traditional news channels don't use the same algorithms that social media algorithms do, restricting the development of algorithmic biases, echo chambers and filter bubbles (Rhodes, 2021; Bartley et al., 2021; Du, 2023; Liao, 2023).

The "*Regulated Channel, Official Entity*" group combines formally recognized actors with regulated communication channels, potentially enhancing the perceived validity of their messages (Gálik & Tolnaiová, 2022; Balod & Hameleers, 2021; BasuThakur & De, 2023, Chadwick, 2022). Nevertheless, in societies with pervasive distrust of institutions, even this combination might not guarantee message credibility (Bauer, 2021; Zimmermann and Kohring, 2020; Bennet & Livingston, 2018).

The overall trustworthiness of a message is subjective (Maloney, 2024), heavily influenced by the audience's perception (Bearth & Siegrist, 2022), which hinges not just on the message's content (MacKay et al., 2023) but also on the medium used (Sanchez & Baselga, 2023; Chadwick, 2022) and the status of the communicator (Gálik & Tolnaiová, 2022; Balod & Hameleers, 2021; Bearth & Siegrist, 2022). In examining the interaction between audience vulnerabilities and message delivery channels, it becomes evident that different vulnerability profiles exhibit varying susceptibilities. Individuals with a '*Conscious Strong Attachment to Beliefs*' are particularly prone to influence from *Unregulated Official* and *Unregulated Unofficial* groups, often seeking information that reinforces their existing convictions (Kahneman et al., 1982; Nickerson, 1998). Those characterized by '*Conscious Open-Mindedness*' display resiliency, but with potential vulnerability to *Unregulated Official*, albeit with a more critical approach due to their informed decision-making process. The '*Subconscious Strong Attachment to Beliefs*' profile is notably susceptible to the Unregulated Unofficial group, influenced by automatic biases and less discerning information processing. Lastly, the '*Subconscious Open-Mindedness*' profile, with its natural inclination towards diverse viewpoints, shows vulnerability to a broad spectrum of groups, including *Unregulated Official* and *Unregulated Unofficial*, highlighting the trust factors significance in digital communication across different audience segments.

5.2.3 Audience

The audience, comparative to Wardle's (2017) interpreter, pertains to the individuals receiving or observing digital communication, whose actions are targeted for manipulation. The literature review illustrated that various factors contribute to these vulnerabilities, including demographics, cultural background, educational levels (or lack thereof), personal experiences, and more.

Individuals often form initial decisions based on limited information or a single narrative, but typically seek additional data subsequently (Endsley, 2018). This pursuit, driven by specific goals and deliberate processing, usually aims to find news stories that align with and reinforce pre-existing beliefs or expectations within their cognitive frameworks (Kahneman et al., 1982; Nickerson, 1998). Nonetheless, when these preconceptions are erroneous, confirmation bias leads people to favor information that supports their existing viewpoints, while overlooking or minimizing evidence to the contrary (Nickerson, 1998). Attacks on information aim to undermine confidence in information; thus, when individuals encounter uncertainty or misinformation online, their ability to comprehend and utilize information is significantly impaired (Endsley, 2018). This impairment results in delayed information processing and decision-making, even when accurate information is available. Ultimately, integrating new information with existing knowledge is crucial for developing a coherent understanding. If new information corroborates existing beliefs, it is readily accepted. Conversely, when new information contradicts these beliefs, individuals are likely to either reject this information or seek justifications to align it with their current, albeit incorrect, beliefs (Nickerson, 1998).

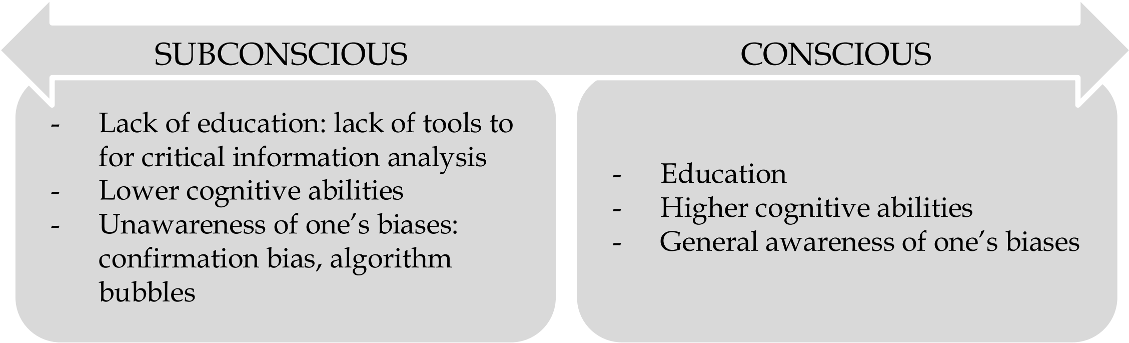
To effectively analyze these attributes, a grid was created by intersecting two continua. One continuum spans from conscious to subconscious, while the other extends from a strong attachment to beliefs to open-mindedness.

5.2.3.1 Subconscious – Conscious

The literature review suggested various variables to consider when examining one's vulnerability in the context of digital communication. The conscious mind, propelled by factors such as education, cognitive abilities, and awareness, is directed towards an analysis of information and discerning engagement with digital content (Moussa et al., 2022; Paisana et al., 2020). In contrast, the subconscious domain introduces automatic processes and latent biases that subtly impact perceptions and reactions (Levendusky, 2013). Central to conscious involvement in the digital landscape is formal education, providing individuals with tools for critical information analysis, source identification, and the discernment between fact and fiction (Hwang and Jeong ,2023). Education serves as a foundational element, fostering a conscious approach that enables individuals to navigate the digital realm with heightened scrutiny and discernment. For instance, sociodemographic variables, such as age group, nationality and level of education & possible major's, disabilities and social exclusion significantly affect the ability to identify and perceive information. (Moussa et al., 2022; Paisana et al., 2020; Elers, 2023, Crucian, 2023; Quintanilha, 2018.)

Cognitive capabilities play a crucial role in shaping the conscious dimension of this continuum. Individuals with higher cognitive skills are more aware of fake news, and are thus able to discern them from real news (Pennycook & Rand, 2019). Higher cognitive ability is linked to better information processing and decision-making skills (Lodge and Hamill, 1986; Gonzalez et al., 2005; Taber and Lodge, 2006): enhanced cognitive abilities empower individuals to process complex information, engage in critical thinking, and make nuanced decisions. These capabilities contribute to a purposeful effort in evaluating online content, considering diverse perspectives, and making well-informed choices within the digital landscape (Mitchell et al., 2018; Van Duyn & Collier, 2019; Taber and Lodge, 2006). However, it's noteworthy to mention that there's times when disinformation slips through people's conscious screening (Rhodes, 2021). Overall, individuals with higher cognitive abilities have been found to show more skepticism when exposed to false content compared to those with lower cognitive abilities (Ahmed, 2023; Qahri-Saremi & Turel, 2023).

Awareness serves as a vital conduit connecting the conscious and subconscious realms. A general awareness of one's biases, an understanding of the dynamics of the digital landscape (Shi et al., 2022), and recognition of the prevalence of misinformation enhance an individual's ability to navigate digital communication consciously (Qahri-Saremi & Turel, 2023; Endsley, 2018), Instilling a sense of responsibility in critically evaluating online information. However, awareness can be affected by situational factors such as poor sleep quality, social media ostracism, source likeability and fear appeals (Qahri-saremi & Turel, 2023; Graziano & Percoco, 2017). Sometimes people can restrain themself from clicking on a phishing message, overrunning the need for immediate gratification, if their *motivation* and *abilities* are strong enough (Collins, 1992; Baumeister, 2002; Eyal, 2014; Milyavskaya, 2015; Moody, 2011; Chadwick, 2022). Formal education establishes the groundwork for conscious engagement, while cognitive capabilities refine the decision-making process (Paisana et. al., 2020). Awareness, continually nurtured through education and self-reflection, functions as a resilient buffer against the subtle influences of subconscious biases.



- Lack of education: lack of tools to for critical information analysis
- Lower cognitive abilities
- Unawareness of one’s biases: confirmation bias, algorithm bubbles

- Education
- Higher cognitive abilities
- General awareness of one’s biases

FIGURE 4 Subconscious – Conscious continuum

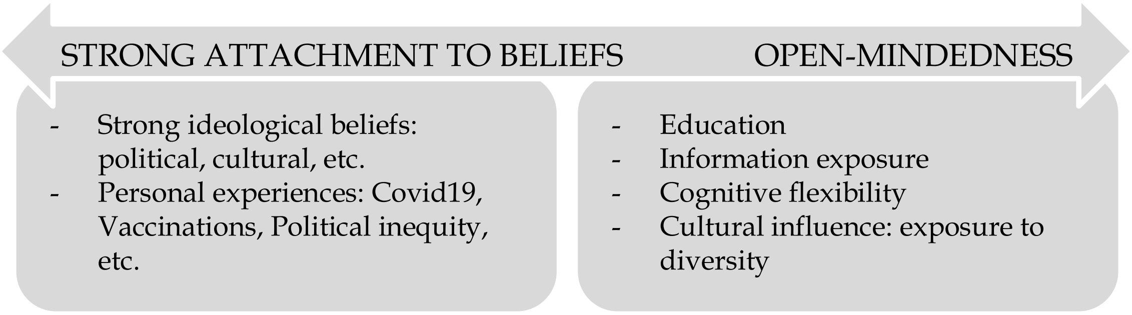
5.2.3.2 Strong Attachment to Beliefs – Open-Mindedness

Information polarization, confirmation biases and echo chambers were highlighted in the literature review. Individuals firmly grounded in personal convictions navigate the digital landscape through a lens shaped by their held beliefs, rooted in personal values and cultural influences (Nikcerson, 1998; Bartley et al., 2021; Sanchez and Baselga, 2023; Bauer & Clemm von Hohenberg, 2021). Because social media platforms are designed to hook people on them, keep them engaged by creating highly personalized content, these beliefs act as filters, interpreting incoming information which then becomes homogeneous as people consciously choose to follow people who share the same ideologies, avoiding information that contradicts their existing views, thus creating filter bubbles and echo chambers (Stubenvoll et al., 2021; Nickerson, 1998, Rhodes, 2021). Conversely, the minority of individuals characterized by open-mindedness explore the digital realm with a spirit of curiosity. Their receptivity to diverse perspectives fosters a nuanced understanding of information, encouraging the scrutiny of preconceived notions and a dynamic engagement with evolving digital discourse (Moussa et al., 2022; Masip et al., 2020).

Numerous factors intricately shape an individual's position on the "*Strong Attachment to Beliefs – Open-mindedness*" continuum: cultural background, personal experiences, education and information exposure, and cognitive flexibility (Moussa et al., 2022; Paisana et al., 2020; Tsfati et al., 2020; Sanchez and Baselga, 2023; Rhodes, 2021; Quintanilha, 2018; Maloney, 2024).

Cultural influences mould personal beliefs, determining the degree of attachment to specific ideologies (Levendusky, 2013; Maloney, 2024). Nevertheless, exposure to diverse cultures can cultivate open-mindedness by fostering an appreciation for different perspectives. Past experiences contribute to the formation of personal beliefs, anchoring individuals in specific convictions. Varied experiences can promote open-mindedness by exposing individuals to a spectrum of viewpoints. Formal education and exposure to specific information sources can either reinforce or challenge existing beliefs (Crucian, 2023). On the contrary, a diverse education and exposure to a range of information sources can also broaden perspectives and enhance open-mindedness (Rhodes, 2021). Cognitive flexibility enables individuals to adapt their beliefs based on new information. Greater cognitive flexibility fosters a more open-minded approach to navigating the digital landscape (Bearth & Siegrist, 2022).

The interplay between personal beliefs and open-mindedness is a dynamic process. Striking a balance necessitates a conscious recognition of the influence of cultural background, personal experiences, education, and cognitive flexibility on one's position along the continuum (Rhodes, 2021). Achieving this balance ensures a nuanced and enriched digital engagement. In the dynamic landscape of digital communication, comprehending the interplay between a strong attachment to beliefs and open-mindedness is crucial. By acknowledging the impact of personal attributes, individuals can cultivate a thoughtful approach, fostering a digital environment that promotes dialogue, embraces diversity, and appreciates the ever-evolving nature of knowledge.



STRONG ATTACHMENT TO BELIEFS

- Strong ideological beliefs: political, cultural, etc.
- Personal experiences: Covid19, Vaccinations, Political inequity, etc.

OPEN-MINDEDNESS

- Education
- Information exposure
- Cognitive flexibility
- Cultural influence: exposure to diversity

FIGURE 5 Strong attachment to Beliefs – Open-mindedness continuum

5.2.3.3 Audience types

The previous continua are intersected, resulting in the formation of a grid. This grid delineates four distinct quadrants: "*Conscious Strong Attachment to Beliefs,*" "*Subconscious Strong Attachment to Beliefs,*" "*Conscious Open-Mindedness,*" and "*Subconscious Open-Mindedness.*" These quadrants are subsequently elucidated by delineating their primary attributes, thus establishing specific profiles. Individuals situated in the quadrant of "*Conscious Strong Attachment to Beliefs*" exhibit a vulnerability profile referred to as "*Belief-Driven Guardians*." These individuals, deeply engaged in the digital realm, demonstrate a robust adherence to their personal beliefs and convictions. Their interpretive frameworks and decision-making processes are significantly shaped by their entrenched values and cultural influences. These individuals proactively pursue information that aligns with their ideological stance.

Conversely, individuals placed in the "*Conscious Open Minded*" quadrant are characterized as "*Practical Decision-Makers.*" They actively seek information but maintain a willingness to expand their perspectives and knowledge base. Their educational experiences have equipped them with critical analytical skills, enabling them to consider diverse viewpoints. Their decision-making is marked by well-reasoned and informed judgements. The "*Subconscious Strong Attachment to Beliefs*" quadrant includes individuals whose innate thought processes are intrinsically aligned with their personal beliefs. Termed "*Unconscious Anchors,*" these individuals' perceptions and reactions are subtly influenced by underlying biases. This often results in one or the other outcomes. An involuntary leaning towards specific convictions, occurring without their conscious awareness. Or a cognitive mechanism avoiding ostracism, ghosting or FOMO.

Lastly, individuals identified as "*Innately Open Explorers*'' in the "*Subconscious Open Minded*" quadrant display a natural inclination towards open-mindedness, driven by unconscious thought processes. Influences such as cultural exposure, varied life experiences, and mental flexibility contribute to their spontaneous receptiveness to differing viewpoints.

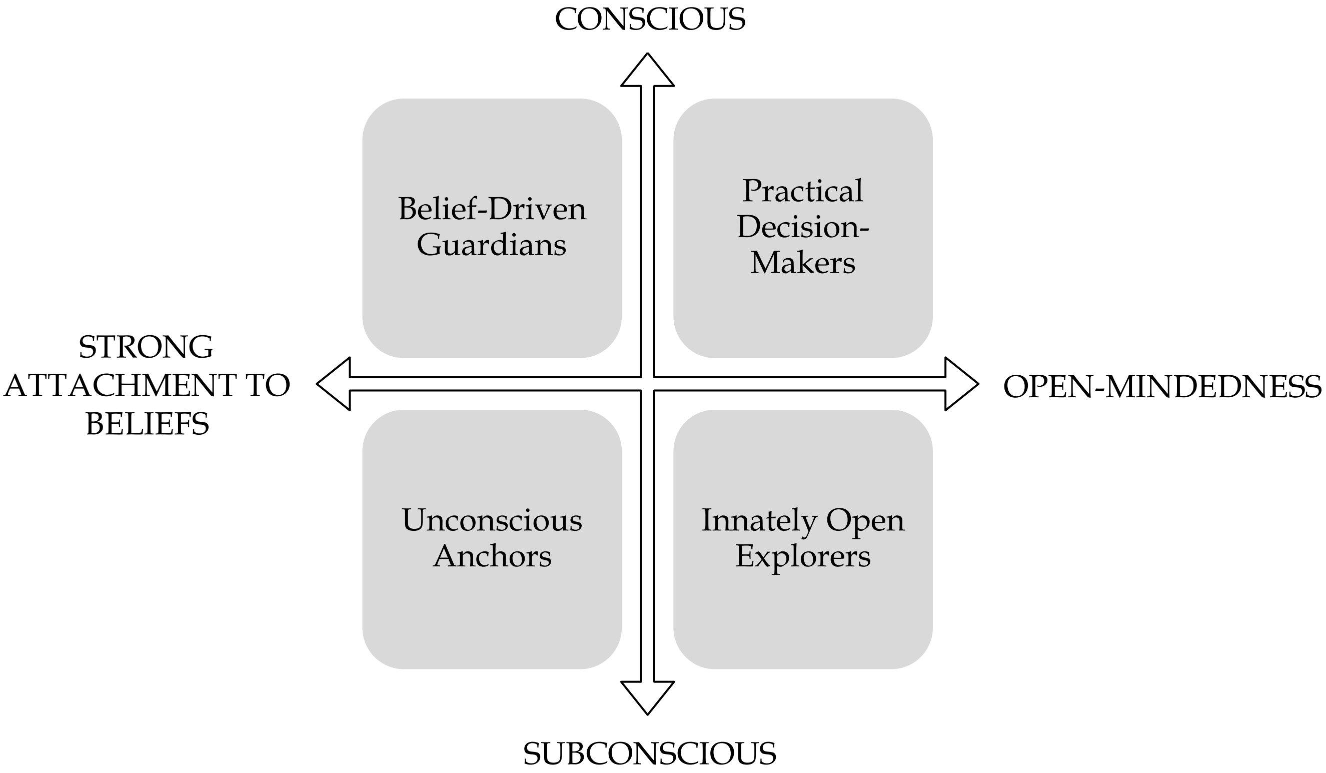


FIGURE 6 Audience types

TABLE 12 Audience types

Profile	Description	Attributes
Belief-Driven Guardians *Individuals positioned in the "Conscious Strong Attachment to Beliefs" quadrant.*	Individuals navigating the digital landscape with a deeply rooted attachment to personal convictions and beliefs. Their conscious approach, shaped by strong values and cultural influences, serves as a filter for interpreting incoming information.	High cultural attachment, strong ideological beliefs, great potential for confirmation bias.
Practical Decision-Makers *Individuals located in the "Conscious Open-Mindedness" quadrant.*	Individuals approaching the digital realm with a conscious and deliberate open-mindedness. Formally educated, they actively engage in critical thinking, considering diverse perspectives, and making well-informed choices.	Formal education, enhanced cognitive abilities, active awareness, conscious open-mindedness.
Unconscious Anchors *Individuals situated in the "Subconscious Strong Attachment to Beliefs" quadrant.*	Individuals whose subconscious processes strongly align with personal beliefs. Automatic biases subtly influence their perceptions and reactions, often leading to an unconscious anchoring in specific convictions.	Subconscious biases, automatic alignment with beliefs, potential for unintentional confirmation bias.
Innately Open Explorers *Individuals positioned in the "Subconscious Open-Mindedness" quadrant.*	Individuals whose subconscious processes naturally foster open-mindedness. Cultural influences, diverse experiences, and cognitive flexibility contribute to an innate receptivity to different perspectives.	Cultural diversity, varied experiences, cognitive flexibility, natural openness to diverse viewpoints.

5.2.4 Framework Elements' Overlap

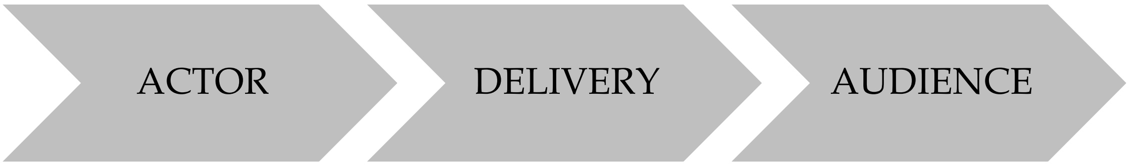


FIGURE 7 Framework elements

To conclude, the framework breaks down the aspects of vulnerability and exploitation in digital communication into three main elements: **actor**, **audience**, and **delivery**. These elements are distinct and can be analyzed separately: the actor is evaluated based on their intent to cause harm, their motivation, and attack vector; the audience is looked at in terms of how they perceive the message and the factors influencing this perception; and delivery focuses on the channel and the entity disseminating the message. However, upon closer examination and breaking these elements down into smaller parts, it becomes apparent that there is an overlap among the three main elements.

The actor is defined as the producer behind the harm distributed through means of digital communication. In the process of examining the base elements of vulnerabilities and their exploitation, the actor is its own element. However, in the process of message distribution, it is not necessarily separate from the audience and the delivery. For example, the actor can be the official or unofficial entity examined in the delivery, or an unintentional actor can originate from the audience when spreading harmful misinformation.

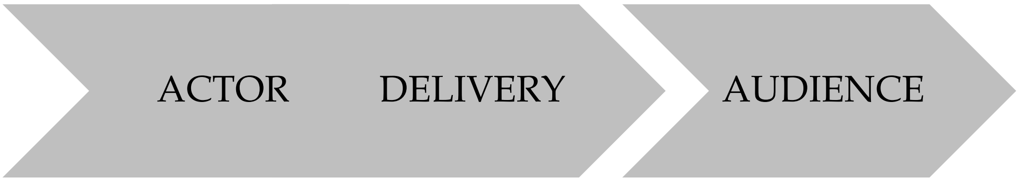


FIGURE 8 Framework elements overlap

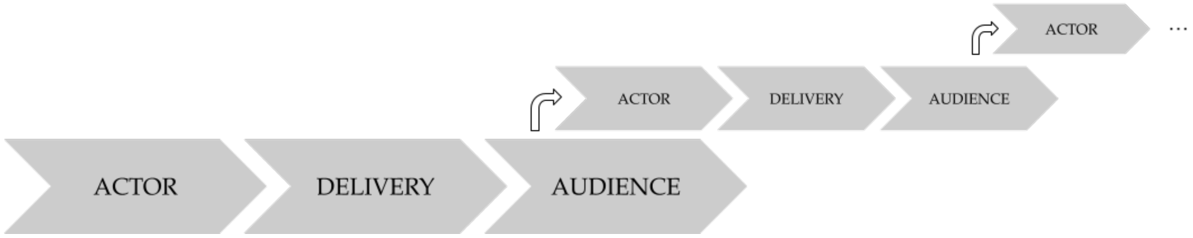


FIGURE 9 Framework elements overlap

6 VULNERABILITY FRAMEWORK

The final framework is conducted from the components explored above. The first layer, **attack vector**, involves analyzing the actor, their motives, and the means of exploitation. The **audience type** layer focuses on assessing audience susceptibilities and the factors influencing them, leading to the formation of four distinct types. The last layer, **credibility variables**, explores the specific contexts or environments where these vulnerability profiles are most susceptible to influence or attack. This layered approach provides a comprehensive understanding of the vulnerabilities in digital communication.

Fundamentally, the vulnerability resides within the profiles, while the arena serves as the gateway. It is vital to examine how each profile engages with different parts of the arena, this being the way to determine where they are susceptible.

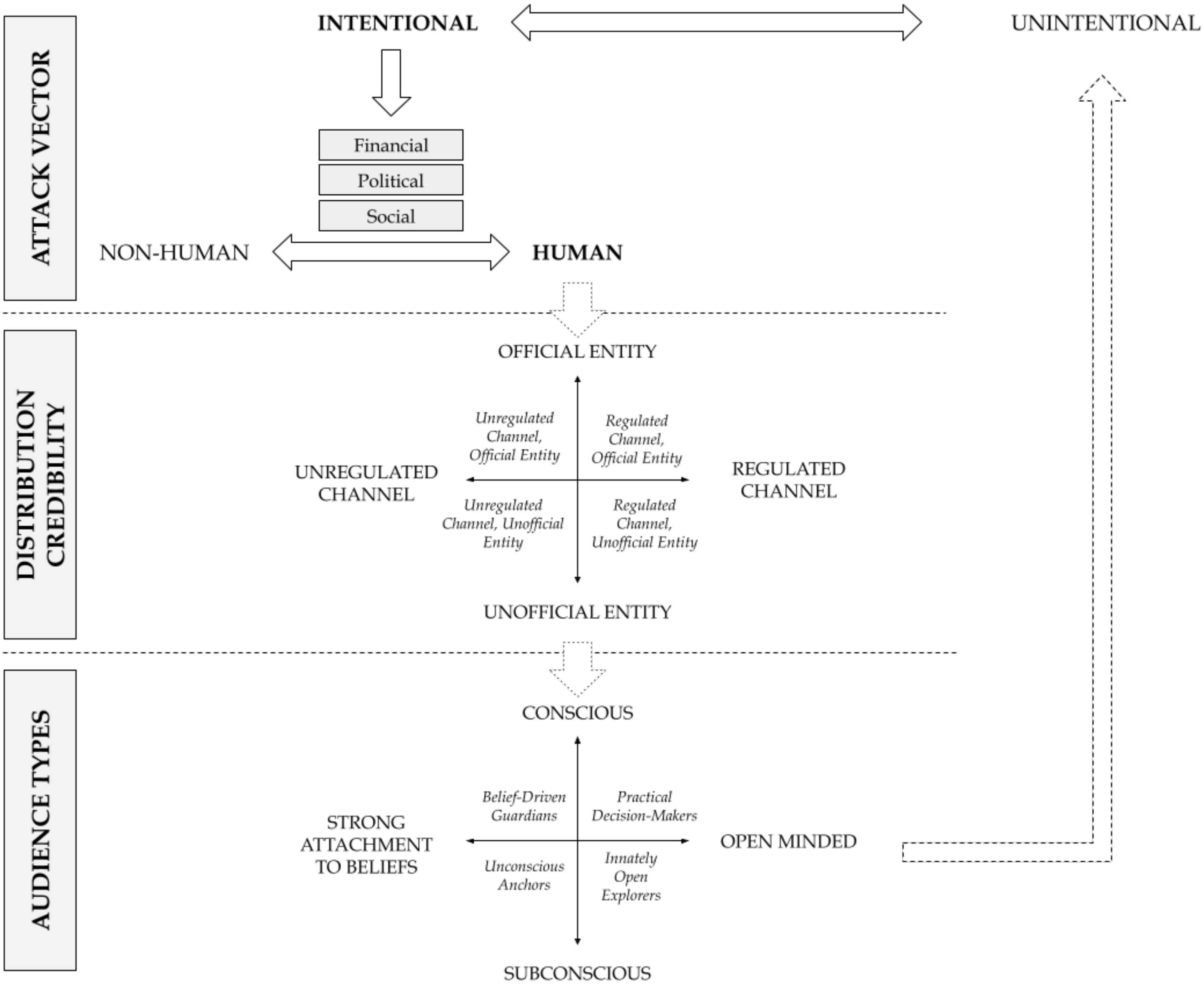


FIGURE 10 Vulnerability Framework

In the following chapter some examples on how different audience types are vulnerable to harm such misinformation and disinformation.

Belief-Driven Guardians who consume like-minded media, will become more extreme in their beliefs and start to use motivated reasoning in order to stomp any counterarguments, even if they don’t remember all of the facts presented earlier (Levendusky, 2013). This is fueled by partisan media and algorithms, leading these people to view fake news as more believable (Rhodes, 2021). Furthermore, as these ideological media bubbles become the "norm" for these individuals, their chosen medium for news content further deepens the ideology by leaving out misinformation corrections (Maloney, 2018). Thus, their ideology grows stronger, and differing views on social media and news are starting to look like disinformation for them. For example, presenting scientifically backed arguments for COVID-19 behavior does not necessarily influence people who have their own strong beliefs opposing behavior changes that the pandemic calls for (Sanchez & Baselga, 2023). In some cases, the Belief-

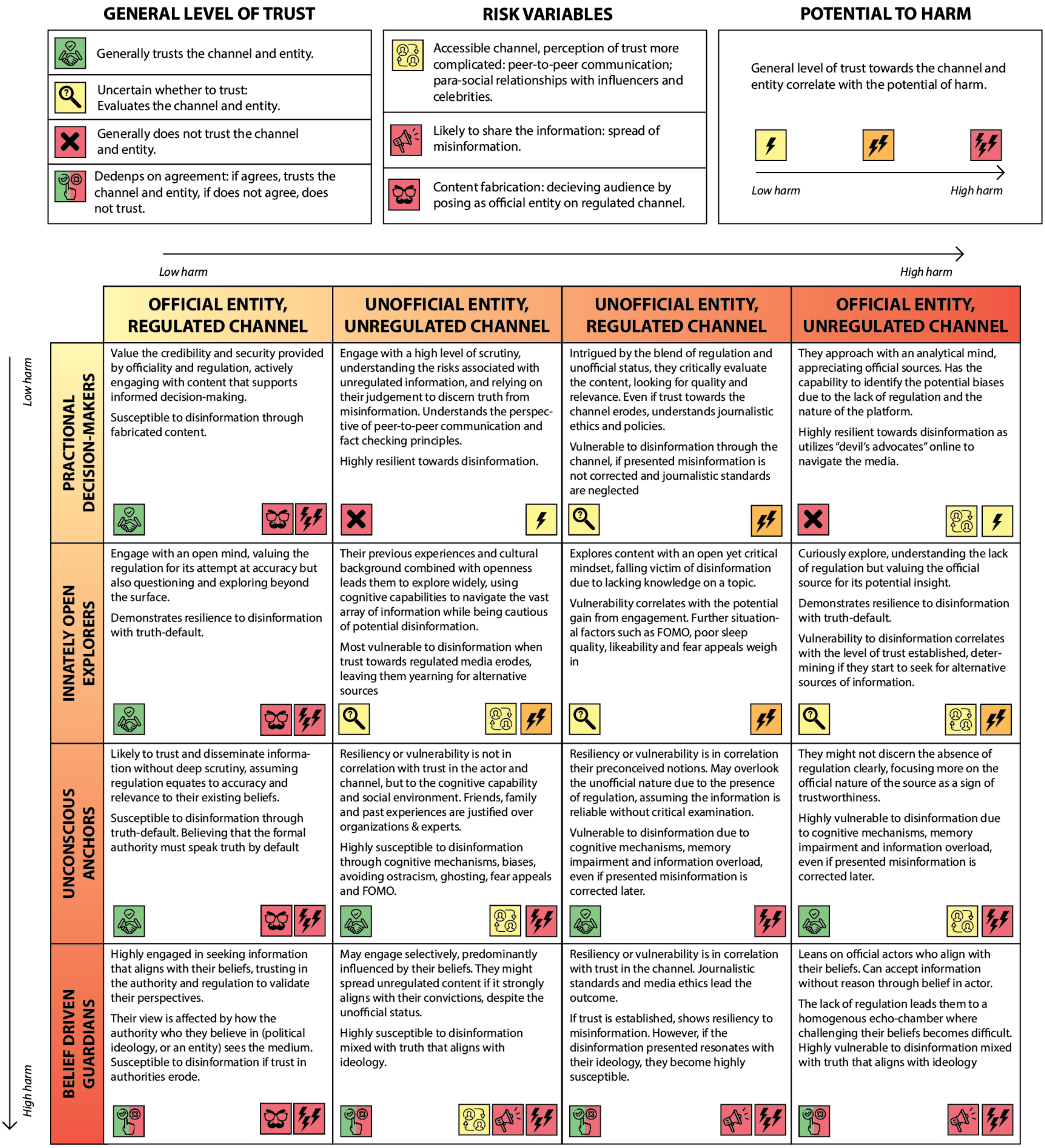
Driven Guardians simply do not care if the information is wrong, as they believe in the authority or cause behind it.

Practical Decision-Makers have the cognitive capability to know that the online environment is flooded with misinformation and to read news that promote opposing views (Rhodes, 2021; Ahmed, 2023). Once they identify something as a "trust heuristic", it supports reasoning in uncertain situations without many resources from the individual making the decision, allowing them to judge information sources and trust in regulators (Bearth & Siegrist, 2022). As they show higher levels of trust towards official news sources, they expose themselves to less misinformation/disinformation online, making their "own truth" from the available information through practical decision making (Ahmed, 2023; Moussa, 2022; Rhodes, 2021).

Unconscious Anchors fall victim for cognitive biases, leaning towards information that sounds more believable even though it's the result from a confirmation/disconfirmation bias (Nickerson, 1998) For example, their biases may be activated through social acceptance, where in uncertain situations the bias pushes them towards misinformation as that makes them seem socially accepted in a certain group and thus avoid online ostracism (Bearth & Siegrist, 2022; Qahri-Saremi, 2023). Another way of triggering a bias is through tv-media, as people can be swayed to vote for coalitions supporting crime prevention by showing amounts of crime on tv (Graziano & Percoco, 2016).

Innately Open Explorers are exposed to misinformation, when they lose trust towards regulated media and begin searching for alternative sources (Zimmermann & Kohring, 2020).

To understand these vulnerabilities, a figure was created about audience types on distribution credibility, highlighting the vulnerabilities that different profiles have on different arenas. While similarities in the profiles can be found, differences from one another vary on how much harm potential there is. For example, on the bottom-right corner *Belief Driven Guardians* are most vulnerable on the *Official Actor, Unregulated Channel* arena. In contrast, top-left corner of *Practical Decision-Makers* are most resilient on the *Official Actor, Regulated Channel.*



GENERAL LEVEL OF TRUST	
🤝	Generally trusts the channel and entity.
🔍	Uncertain whether to trust: Evaluates the channel and entity.
✖	Generally does not trust the channel and entity.
☝	Dedenps on agreement: if agrees, trusts the channel and entity, if does not agree, does not trust.

RISK VARIABLES	
👥	Accessible channel, perception of trust more complicated: peer-to-peer communication; para-social relationships with influencers and celebrities.
📢	Likely to share the information: spread of misinformation.
🎭	Content fabrication: decieving audience by posing as official entity on regulated channel.

POTENTIAL TO HARM

General level of trust towards the channel and entity correlate with the potential of harm.

⚡ → ⚡⚡ → ⚡⚡⚡

Low harm → *High harm*

Low harm → *High harm* (columns)

Low harm ↓ *High harm* (rows)

	OFFICIAL ENTITY, REGULATED CHANNEL	UNOFFICIAL ENTITY, UNREGULATED CHANNEL	UNOFFICIAL ENTITY, REGULATED CHANNEL	OFFICIAL ENTITY, UNREGULATED CHANNEL
PRACTIONAL DECISION-MAKERS	Value the credibility and security provided by officiality and regulation, actively engaging with content that supports informed decision-making. Susceptible to disinformation through fabricated content. 🤝 🎭 ⚡⚡⚡	Engage with a high level of scrutiny, understanding the risks associated with unregulated information, and relying on their judgement to discern truth from misinformation. Understands the perspective of peer-to-peer communication and fact checking principles. Highly resilient towards disinformation. ✖ ⚡	Intrigued by the blend of regulation and unofficial status, they critically evaluate the content, looking for quality and relevance. Even if trust towards the channel erodes, understands journalistic ethics and policies. Vulnerable to disinformation through the channel, if presented misinformation is not corrected and journalistic standards are neglected 🔍 ⚡⚡	They approach with an analytical mind, appreciating official sources. Has the capability to identify the potential biases due to the lack of regulation and the nature of the platform. Highly resilient towards disinformation as utilizes “devil’s advocates” online to navigate the media. ✖ 👥 ⚡
INNATELY OPEN EXPLORERS	Engage with an open mind, valuing the regulation for its attempt at accuracy but also questioning and exploring beyond the surface. Demonstrates resilience to disinformation with truth-default. 🤝 🎭 ⚡⚡⚡	Their previous experiences and cultural background combined with openness leads them to explore widely, using cognitive capabilities to navigate the vast array of information while being cautious of potential disinformation. Most vulnerable to disinformation when trust towards regulated media erodes, leaving them yearning for alternative sources 🔍 👥 ⚡⚡	Explores content with an open yet critical mindset, falling victim of disinformation due to lacking knowledge on a topic. Vulnerability correlates with the potential gain from engagement. Further situational factors such as FOMO, poor sleep quality, likeability and fear appeals weigh in 🔍 ⚡⚡	Curiously explore, understanding the lack of regulation but valuing the official source for its potential insight. Demonstrates resilience to disinformation with truth-default. Vulnerability to disinformation correlates with the level of trust established, determining if they start to seek for alternative sources of information. 🔍 👥 ⚡⚡
UNCONSCIOUS ANCHORS	Likely to trust and disseminate information without deep scrutiny, assuming regulation equates to accuracy and relevance to their existing beliefs. Susceptible to disinformation through truth-default. Believing that the formal authority must speak truth by default 🤝 🎭 ⚡⚡⚡	Resiliency or vulnerability is not in correlation with trust in the actor and channel, but to the cognitive capability and social environment. Friends, family and past experiences are justified over organizations & experts. Highly susceptible to disinformation through cognitive mechanisms, biases, avoiding ostracism, ghosting, fear appeals and FOMO. 🤝 👥 ⚡⚡⚡	Resiliency or vulnerability is in correlation their preconceived notions. May overlook the unofficial nature due to the presence of regulation, assuming the information is reliable without critical examination. Vulnerable to disinformation due to cognitive mechanisms, memory impairment and information overload, even if presented misinformation is corrected later. 🤝 ⚡⚡⚡	They might not discern the absence of regulation clearly, focusing more on the official nature of the source as a sign of trustworthiness. Highly vulnerable to disinformation due to cognitive mechanisms, memory impairment and information overload, even if presented misinformation is corrected later. 🤝 👥 ⚡⚡⚡
BELIEF DRIVEN GUARDIANS	Highly engaged in seeking information that aligns with their beliefs, trusting in the authority and regulation to validate their perspectives. Their view is affected by how the authority who they believe in (political ideology, or an entity) sees the medium. Susceptible to disinformation if trust in authorities erode. ☝ 🎭 ⚡⚡⚡	May engage selectively, predominantly influenced by their beliefs. They might spread unregulated content if it strongly aligns with their convictions, despite the unofficial status. Highly susceptible to disinformation mixed with truth that aligns with ideology. ☝ 👥 📢 ⚡⚡⚡	Resiliency or vulnerability is in correlation with trust in the channel. Journalistic standards and media ethics lead the outcome. If trust is established, shows resiliency to misinformation. However, if the disinformation presented resonates with their ideology, they become highly susceptible. ☝ 📢 ⚡⚡⚡	Leans on official actors who align with their beliefs. Can accept information without reason through belief in actor. The lack of regulation leads them to a homogenous echo-chamber where challenging their beliefs becomes difficult. Highly vulnerable to disinformation mixed with truth that aligns with ideology ☝ 📢 ⚡⚡⚡

FIGURE 11 Audience Types on Distribution Credibility

Figure 11 illustrates the perceptions of audience segments regarding the distribution of information involved in the dissemination of information. It employs icons at the bottom of each matrix cell to denote the general trust level, risk factors, and potential harm associated with each audience type. The potential of harm correlates with the general level of trust towards the channel and entity: if one usually trusts in one and is then deceived, the done harm is more significant.

The categorization of dissemination variables is sequenced as follows: Official Entity, Regulated Channel; Unofficial Entity, Unregulated Channel; Unofficial Entity, Regulated Channel; and Official Entity, Unregulated Channel. This sequencing is predicated upon an assessment of their inherent trustworthiness and the potential for deception. The combination of an Official Entity operating through a Regulated Channel is deemed to embody the pinnacle of reliability, a conclusion that is logically cogent. Most audience types place their confidence in communications propagated via this conduit and entity. An exception exists in the form of Belief-Driven Guardians, who predicate their trust on the congruence of the message with their pre-existing convictions. Nevertheless, when the message corroborates their beliefs, they leverage the official and regulated nature of the channel to substantiate their perspective. Conversely, discordance with the message results in a complete negation of the entity's and channel's credibility.

The primary risk associated with the Official Entity operating through a Regulated Channel lies in the potential for audiences to be deceived by fabricated content. Given the inherent trust placed in this medium, a successful deception can lead numerous individuals to become unwitting victims, predicated on their accustomed reliance on the credibility of this source.

Notably, the Unofficial Entity, Unregulated Channel is predominantly associated with the proliferation of misinformation, recognized by audiences as lacking in credibility due to its facilitation of peer-to-peer exchanges. The principal risk associated with this channel emanates from the formation of parasocial interactions, leading individuals to ascribe credibility to celebrities and social media influencers undeservedly.

The credibility attributed to the Unofficial Entity, Regulated Channel derives from its regulated status, suggesting to audiences that it has undergone several layers of regulatory scrutiny, so trust on the entity is also built.

The combination of an Official Entity and an Unregulated Channel poses the greatest potential for harm. Despite the credibility typically ascribed to Official Actors, their engagement with audiences through unregulated platforms alters the dynamics of influence and trust, primarily due to the resurgence of parasocial interactions, thereby enabling Official Actors to further their objectives.

7 DISCUSSION AND IMPLICATIONS

This final chapter concludes the findings of the study with the objective of answering the research questions posed and discussing its theoretical and managerial contributions. An evaluation of the study is conducted, considering its trustworthiness and any limitations encountered. Lastly, suggestions for future research are provided.

7.1 Conclusions

> **RQ1:** In what ways can digital communication be vulnerable?

The thesis identifies multiple dimensions of vulnerabilities in digital communication, emphasizing not just the technological weaknesses but also socio-technical challenges such as misinformation dissemination, privacy concerns, and the manipulation of digital platforms for nefarious purposes. These vulnerabilities stem from a combination of technological gaps, policy failures, human behavior, and systemic issues within digital ecosystems. Losing trust in the actor is found to be the most important factor in exposing oneself to misinformation.

> **RQ2:** What framework can be employed to define and categorize vulnerabilities of digital communication?

The proposed framework in the thesis systematically categorizes digital communication vulnerabilities by integrating both the source and impact of these vulnerabilities. It uses a holistic approach that includes technical aspects (such as security flaws and system design issues) and human factors (such as user behavior and organizational policies), offering a nuanced perspective that aids in the comprehensive understanding and mitigation of vulnerabilities.

7.2 Theoretical Contributions

This study enhances understanding of digital communication vulnerabilities, contributing to theory by categorizing these vulnerabilities and their impacts on information integrity and stakeholder trust. By systematically reviewing literature, it introduces a comprehensive framework that identifies gaps in current research, suggesting areas for future study. This work underscores the complexity of digital ecosystems and the multifaceted nature of online threats, urging a reevaluation of existing theories on digital trust and security within the context of rapid technological advancements.

7.3 Managerial Contributions

From a managerial standpoint, this research outlines actionable strategies for mitigating digital vulnerabilities, emphasizing the importance of robust cybersecurity protocols, ongoing employee training, and public awareness campaigns on media literacy. It advocates for a proactive approach to digital communication management, highlighting the necessity of transparency and ethical practices in building stakeholder trust. Furthermore, it calls for policymakers to craft regulations that address the evolving landscape of digital threats, ensuring organizations can navigate these challenges effectively while safeguarding user data and maintaining operational integrity.

7.4 Evaluation: Trustworthiness & Limitations

Systematic review aims to "comprehensively locate and synthesize research that bears on particular questions, using organized. transparent, and replicable procedures at each step in the process" (Littell et al. 2008, p. 1). This contrasts with a "narrative" approach, which tends to be rather descriptive as they do not discuss the methodology used to evaluate the included scholarly papers and lack proper inclusion and exclusion criteria (Palmatier et al. 2018). This study succeeded in replicability in the research process, as the steps taken are described and thus followable. Given the involvement of two researchers in this thesis, the process of selecting articles for inclusion was conducted through dual examination, ensuring each article was reviewed by both researchers to enhance the thoroughness and reliability of the selection. The criteria for inclusion and exclusion in this study are explicitly delineated; however, it is important to acknowledge that there remains a potential for subjective judgement within these parameters, necessitating recognition of this aspect in the evaluation process.

Chapter 4, titled "Results," presents an analysis of the articles encompassed in the systematic literature review. The categorization of these articles is based on key terms as identified by the authors, a method that carries certain limitations. Primarily, the thematic grouping introduces a degree of subjectivity. Nonetheless, the replicability of this process is supported by the explicit listing of key terms for each group within the thesis. It is important to note that this approach heavily relies on the key terms provided by the original authors of the articles, thereby reflecting their interpretation of the most relevant aspects of their studies. This reliance may not fully align with the objectives of this study.

7.5 Future Research

Future research could delve into the effectiveness of communication across regulated and unregulated channels, focusing on audience reception to understand optimal messaging strategies. Exploring audience perception dynamics, particularly how trust evolves in response to crises or political changes, offers insight into source credibility. Investigating social media algorithms' role in shaping public opinion and message dissemination could illuminate biases and echo chambers' effects. Cross-cultural studies on communication network credibility could highlight global variations in information processing. Lastly, examining the psychological impacts of exposure to diverse communication networks may reveal deeper insights into misinformation spread and belief systems.

REFERENCES

Ahmed, S. (2023). Navigating the maze: Deepfakes, cognitive ability, and social media news skepticism. New Media & Society, 25(5), 1108–1129. https://doi.org/10.1177/14614448211019198

Antifake. (2022). Psihologia dezinformării: Ce este citirea laterală? https://www.antifake.ro/psihologia-dezinformarii-ce-este-citirea-laterala-2/

Balaskas, S., Panagiotarou, A., & Rigou, M. (2022). The Influence of Trustworthiness and Technology Acceptance Factors on the Usage of e-Government Services during COVID-19: A Case Study of Post COVID-19 Greece. Administrative Sciences, 12(4), 2076-3387. https://doi.org/10.3390/admsci12040129

Balod, H. S., Hameleers, M. (2021). Fighting for truth? The role perceptions of Filipino journalists in an era of mis- and disinformation. Journalism, 22(9), 2368-2385. https://doi.org/10.1177/1464884919865109

Bandy, J. (2021). Problematic Machine Behavior: A Systematic Literature Review of Algorithm Audits. Proceedings of the ACM on human-computer interaction, 5(74), 1-34. https://doi.org/10.1145/3449148

Baptista, C. F. (2022). Transparency in Portuguese media: From the buzzword to the unsolved regulatory challenge. Observatorio (OBS*), 16(2), 138. https://doi.org/10.15847/obsOBS16220221952

Bartley, N., Abeliuk, A., Ferrara, E., & Lerman, K. (2021). Auditing Algorithmic Bias on Twitter. 13th ACM Web Science Conference 2021, 65–73. https://doi.org/10.1145/3447535.3462491

BasuThakur, P., & De, S. (2023). Government communication strategy and its reflection on media construction of pandemic: A structured analysis of COVID-19 in India. Review of Communication, 23(3), 276–292. https://doi.org/10.1080/15358593.2023.2228875

Bauer, P. C., & Clemm von Hohenberg, B. (2021). Believing and Sharing Information by Fake Sources: An Experiment. Political Communication, 38(6), 647–671. https://doi.org/10.1080/10584609.2020.1840462

Baumeister, R. F. (2002). Yielding to Temptation: Self-Control Failure, Impulsive Purchasing, and Consumer Behavior. Journal of Consumer Research, 28(4), 670–676. https://doi.org/10.1086/338209

Bean, H., Hartnett, S. J., Banaei-Kashani, F., Jafarian, H., & Koutsoukos, A. (2022). "Imitation (In) Security" and the Polysemy of Russian Disinformation: A Case Study in How Ira Trolls Targeted U.S. Military Veterans. Rhetoric & Public Affairs, 25(1), 61–92. https://doi.org/10.14321/rhetpublaffa.25.1.0061

Bearth, A., & Siegrist, M. (2022). The Social Amplification of Risk Framework: A Normative Perspective on Trust? Risk Analysis: An International Journal, 42(7), 1381–1392. https://doi.org/10.1111/risa.13757

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. European

Journal of Communication, 33(2), 122–139. https://doi.org/10.1177/0267323118760317

Bernstein, E. S. (2017) Making Transparency Transparent: The Evolution of Observation in Management Theory. Academy of Management Annals 11(1): 217–266, https://www.hbs.edu/faculty/Pages/item.aspx?num=52164

Bjola, C., & Papadakis, K. (2020). Digital propaganda, counterpublics and the disruption of the public sphere: The Finnish approach to building digital resilience. Cambridge Review of International Affairs, 33(5), 638–666. https://doi.org/10.1080/09557571.2019.1704221

Boman, C. D. (2023). Protecting Against Disinformation: Using Inoculation to Cultivate Reactance Towards Astroturf Attacks. Journal of Public Relations Research, 35(3), 162–181. https://doi.org/10.1080/1062726X.2023.2195184

Breves, P., Amrehn, J., Heidenreich, A., Liebers, N., & Schramm, H. (2021). Blind trust? The importance and interplay of parasocial relationships and advertising disclosures in explaining influencers' persuasive effects on their followers. International journal of advertising, 40(7), 1209-1229. https://doi.org/10.1080/02650487.2021.1881237

Brooks, D. J. (2010). What is security: Definition through knowledge categorization. Security journal, 23(3), 225-239. https://doi.org/10.1057/sj.2008.18

Brooks, D. J. (2007) Defining the Science of Security through Knowledge Categorisation. Paper presented at the Criminology and Victimlogical Society of Southern Africa (CRIMSA) Conference, University of Pretoria.

Buchanan, T. (2020) Why do people spread false information online? The effects of message and viewer characteristics on self- reported likelihood of sharing social media disinformation. PLoS ONE. 15(10), e0239666. https://www.doi.org/10.1371/journal.pone.0239666

Calvo, D., Valera-Ordaz, L., Requena i Mora, M., & Llorca-Abad, G. (2022). Fact-checking in Spain: Perception and trust. Catalan Journal of Communication & Cultural Studies, 14(2), 287–305. https://doi.org/10.1386/cjcs_00073_1

Chadwick, A., & Stanyer, J. (2022). Deception as a Bridging Concept in the Study of Disinformation, Misinformation, and Misperceptions: Toward a Holistic Framework. Communication Theory (1050-3293), 32(1), 1–24. https://doi.org/10.1093/ct/qtab019

Chatterjee, S., Chaudhuri, R., & Vrontis, D. (2023). Role of fake news and misinformation in supply chain disruption: impact of technology competency as moderator. Annals of Operations Research, 327(2), 659–682. https://doi.org/10.1007/s10479-022-05001-x

Collins, R. L., & Lapp, W. M. (1992). The Temptation and Restraint Inventory for measuring drinking restraint. British Journal of Addiction, 87(4), 625–633. https://doi.org/10.1111/j.1360-0443.1992.tb01964.x

Comber, B., & Grant, H. (2018). Working Critically and Creatively With Fake News. Journal of Adolescent & Adult Literacy, 62(3), 329–332. https://doi.org/10.1002/jaal.905

Cook, D. J., Mulwor, C. D., & Haynes, R. B. (1997). Systematic reviews: Synthesis of best evidence for clinical decisions. Annals of internal medicine, 126(5), 376-380. https://doi.org/10.7326/0003-4819-126-5-199703010-00006

Craufurd Smith, R., Klimkiewicz, B., & Ostling, A. (2021). Media ownership transparency in Europe: Closing the gap between European aspiration and domestic reality. European Journal of Communication, 36(6), 547-562. https://doi.org/10.1177/0267323121999523

Crucian, N. (2023). The Fake News Phenomenon in the Context of the Covid-19 Pandemic. The Perception of Romanian Students. Journal of Media Research, 16(2), 28–45. https://doi.org/10.24193/jmr.46.2

Cummings, M. L. (2004). Automation bias in intelligent time critical decision support systems. AIAA 3rd Intelligent Systems Conference, Chicago, Illinois, 2004–6313. https://doi.org/10.2514/6.2004-6313

Du, Y. R. (2023). Personalization, Echo Chambers, News Literacy, and Algorithmic Literacy: A Qualitative Study of AI-Powered News App Users. Journal of Broadcasting & Electronic Media, 67(3), 246–273. https://doi.org/10.1080/08838151.2023.2182787

Edwards, M., & Hulme, D. (1996). Too close for comfort? the impact of official aid on nongovernmental organizations. World development, 24(6), 961-973. https://doi.org/10.1016/0305-750X(96)00019-8

Elers, P., Jayan, P., & Dutta, M. J. (2023). Foregrounding digital realities at the locked down raced margins: a culture-centered case study in Aotearoa. Review of Communication, 23(3), 293–307. https://doi.org/10.1080/15358593.2023.2202734

Endsley, M. R. (2018). Combating Information Attacks in the Age of the Internet: New Challenges for Cognitive Engineering. Human Factors, 60(8), 1081–1094. https://doi.org/10.1177/0018720818807357

Eyal, N. (2014). Hooked: How to Build Habit-Forming Products. Penguin.

Fallis, D. (2015). What Is Disinformation? Library Trends, 63(3), 401–426. https://doi.org/10.1353/lib.2015.0014

Farkas, J. (2023). News on fake news: Logics of media discourses on disinformation. Journal of Language & Politics, 22(1), 1–21. https://doi.org/10.1075/jlp.22020.far

Fischer, R. J. & Green, G. (2004) Introduction to Security. Boston, MA: Butterworth-Heinemann

Fourney, A., Racz, M. Z., Ranade, G., Mobius, M., & Horvitz, E. (2017). Geographic and temporal trends in fake news consumption during the 2016 US presidential election. Proceedings of the 2017 ACM conference on information and knowledge management, 2071–2074.

Fox, J., & Haight, L. (2011). Mexico's transparency reforms: Theory and practice. Government Secrecy, 19, 353-379. https://doi.org/10.1108/S0196-1152(2011)0000019022

Freedman, D. (2018). Populism and media policy failure. European journal of communication (London), 33(6), 604-618. https://doi.org/10.1177/0267323118790156

Freelon, D., & Wells, C. (2020). Disinformation as political communication. Political Communication, 37(2), 145–156. https://doi.org/10.1080/10584609.2020.1723755

Gallup. (2016). Confidence in institutions. http://www.gallup.com/poll/1597/confidenceinstitutions.aspx

Gáliks, S., & Tolnaiová, S. G. (2022). Media Coverage and Its Determinants in the Context of the Covid-19 Pandemic. Communication Today, 13(1), 45–58.

Gisondi, M. A., Barber, R., Faust, J. S., Raja, A., Strehlow, M. C., Westafer, L. M., & Gottlieb, M. (2022). A Deadly Infodemic: Social Media and the Power of COVID-19 Misinformation. Journal of medical Internet research, 24(2), e35552. https://doi.org/10.2196/35552

Gongora, S. G., & Ramirez, M. J. E. (2022). Social Cohesion: Mitigating Societal Risk in Case Studies of Digital Media in Hurricanes Harvey, Irma, and Maria. Risk Analysis: An International Journal, 42(8), 1686–1703. https://doi.org/10.1111/risa.13820

Gonzalez, C., Thomas, R. P., & Vanyukov, P. (2005). The relationships between cognitive ability and dynamic decision making. Intelligence (Norwood), 33(2), 169-186. https://doi.org/10.1016/j.intell.2004.10.002

Goldberg, D. P., & Williams, P. (1988). A User's Guide to the General Health Questionnaire. NFER, Nelson, UK.

Goldberg, D. P. (1972). The Detection of Psychiatric Illness by Questionnaire. Maudsley Monograph, 21, Oxford University Press, Oxford.

Gottfried, J., & Shearer, E. (2016). News use across social media platforms 2016. Pew Research Center. http://www.journalism.org/2016/05/26/news-use-across-social-mediaplatforms-2016

Graziano, P. R., & Percoco, M. (2017). Agenda setting and the political economy of fear: How crime news influences voters' beliefs. International political science review, 38(5), 520-533. https://doi.org/10.1177/0192512116656947

Guess, A., Nyhan, B., & Reifler, J. (2018). Inside the fake news bubble? Consumption of online fake news in the 2016 U.S. election [Unpublished manuscript]. https://apo.org.au/sites/default/files/resource-files/2018-01/apo-nid126961.pdf

Haddadi, P., & Besharat, M. A. (2010). Resilience, vulnerability and mental health. Procedia - Social and Behavioral Sciences, 5, 639–642. https://doi.org/10.1016/j.sbspro.2010.07.157

Hansson, S., Orru, K., Siibak, A., Bäck, A., Krüger, M., Gabel, F., & Morsut, C. (2020). Communication-related vulnerability to disasters: A heuristic framework. International Journal of Disaster Risk Reduction, 51, 101931. https://doi.org/10.1016/j.ijdrr.2020.101931

Hameleers, M., Brosius, A., & de Vreese, C. H. (2022). Whom to trust? Media exposure patterns of citizens with perceptions of misinformation and disinformation related to the news media. European Journal of Communication, 37(3), 237–268. https://doi.org/10.1177/02673231211072667

Hardin, R. (1992). The Street-Level Epistemology of Trust. Analyse & Kritik, 14(2), 152–176. https://doi.org/10.1515/auk-1992-0204

Harris, P.L. (2006), Trust. Developmental Science, 10(1), 135-138. https://doi-org.ezproxy.jyu.fi/10.1111/j.1467-7687.2007.00575.x

Heiss, R., von Sikorski, C., & Matthes, J. (2019). Populist Twitter Posts in News Stories: Statement Recognition and the Polarizing Effects on Candidate Evaluation and Anti-Immigrant Attitudes. Journalism practice, 13(6), 742-758. https://doi.org/10.1080/17512786.2018.1564883

Holte, A. J., Fisher, W. N., & Ferraro, F. R. (2022). Afraid of Social Exclusion: Fear of Missing Out Predicts Cyberball-Induced Ostracism. Journal of Technology in Behavioral Science, 7(3), 315–324. https://doi.org/10.1007/s41347-022-00251-9

Humprecht, E., Esser, F., Aelst, P. V., Staender, A., & Morosoli, S. (2023). The sharing of disinformation in cross-national comparison: Analyzing patterns of resilience. Information, Communication & Society, 26(7), 1342–1362. https://doi.org/10.1080/1369118X.2021.2006744

Hussain, S., Melewar, T. C., Priporas, C., Foroudi, P., & Yusef, W. (2021). Understanding Celebrity Trust and Its Effects on Other Credibility and Image Constructs: A Qualitative Approach. Corporate reputation review, 24(4), 247-262. https://doi.org/10.1057/s41299-020-00107-z

Hwang, Y., & Jeong, S.-H. (2023). Misinformation Exposure and Acceptance: The Role of Information Seeking and Processing. Health Communication, 38(3), 585–593. https://doi.org/10.1080/10410236.2021.1964187

James, T. L., Lowry, P. B., Wallace, L., & Warkentin, M. (2017). The Effect of Belongingness on Obsessive-Compulsive Disorder in the Use of Online Social Networks. Journal of Management Information Systems, 34(2), 560–596. https://doi.org/10.1080/07421222.2017.1334496

Jayawickrama, U., Liu, S., Hudson Smith, M., Akhtar, P., & Al Bashir, M. (2019). Knowledge retention in ERP implementations: The context of UK SMEs. Production Planning & Control, 30(10–12), 1032–1047. https://doi.org/10.1080/09537287.2019.1582107

Kahneman, D., Slovic, P., & Tversky, A. (1982). Judgment under uncertainty: Heuristics and biases. Cambridge, UK: Cambridge University Press. Science, 185, 1124-1131 https://doi.org/10.1126/science.185.4157.1124

Katerynych, P. (2022). Comparative analysis of the information security environment in Ukraine and Poland (survey of journalists and editors). Communication & Society, 35(4), 37–53. https://doi.org/10.15581/003.35.4.37-53

Koc-Michalska, K., Klinger, U., Bennett, L., & Römmele, A. (2023). (Digital) Campaigning in Dissonant Public Spheres. Political Communication, 40(3), 255–262. https://doi.org/10.1080/10584609.2023.2173872

Kolker, E. & Kulldorff, C. (2013). Managing Upward and Downward Accountability in an International Development Project - A Case Study of a World Bank Telecommunications Infrastructure Project in Benin, Master's Thesis. Stockholm School of Economics, Department of Management.

Krause, N. M., Freiling, I., & Scheufele, D. A. (2022). The "Infodemic" Infodemic: Toward a More Nuanced Understanding of Truth-Claims and the Need for (Not) Combatting Misinformation. The Annals of the American Academy of Political and Social Science, 700(1), 112-123. https://doi.org/10.1177/00027162221086263

Layton, R., & Duffy, S. (2018). Path Dependency in Marketing Systems: Where History Matters and the Future Casts a Shadow. Journal *of macromarketing, 38*(4), 400-414. https://doi.org/10.1177/0276146718787012

Lazer, D., Baum, M., Grinberg, N., Friedland, L., Joseph, K., Hobbs, W., & Mattsson, CA. (2017). Combating fake news: An agenda for research and action. In Combating fake news conference. Harvard University.

Law, M. (2023). CRISIS & EMERGENCY RISK COMMUNICATION: Six Principles for OSH Professionals. Professional Safety, 68(5), 36–40. https://onepetro.org/PS/article-abstract/68/05/36/519590/Crisis-amp-Emergency-Risk-Communication-Six

Levasseur, M., Lussier-Therrien, M., Biron, M. L., Dubois, M.-F., Boissy, P., Naud, D., Dubuc, N., Coallier, J.-C., Calvé, J., & Audet, M. (2022). Scoping study of definitions and instruments measuring vulnerability in older adults. Journal of the American Geriatrics Society, 70(1), 269–280. https://doi.org/10.1111/jgs.17451

Levendusky, M. (2013). Why Do Partisan Media Polarize Viewers? American Journal of Political Science, 57(3), 611-623. https://onlinelibrary.wiley.com/doi/10.1111/ajps.12008

Li, K., & Shin, D. (2023). Correcting E-Cigarette Misinformation on Social Media: Responses from UAE Nationals Who Smoke. Journal of Broadcasting & Electronic Media, 67(3), 376–396. https://doi.org/10.1080/08838151.2023.2201506

Littell, J. H., Corcoran, J., & Pillai, V. (2008). Systematic reviews and meta-analysis. New York: Oxford University Press.

Lodge, M., & Hamill, R. (1986). A Partisan Schema for Political Information Processing. The American political science review, 80(2), 505-519. https://doi.org/10.2307/1958271

Liao, M. (2023). Understanding the Effects of Personalized Recommender Systems on Political News Perceptions: A Comparison of Content-Based, Collaborative, and Editorial Choice-Based News Recommender System. Journal of Broadcasting & Electronic Media, 67(3), 294–322. https://doi.org/10.1080/08838151.2023.2206662

Lima Quintanilha, T., Torres da Silva, M., & Lapa, T. (2019). Fake news and its impact on trust in the news. Using the Portuguese case to establish lines of differentiation. Communication & Society, 32(3), 17-33. https://doi.org/10.15581/003.32.3.17-33

Luoma-aho, V., & Badham, M. (2023). Handbook on Digital Corporate Communication. Edward Elgar Publishing.

Luoma-aho, V., & Canel, M.-J. (2020). Introduction to Public Sector Communication. In The Handbook of Public Sector Communication (pp. 1–25). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119263203.ch0

MacKay, M., Thaivalappil, A., McWhirter, J. E., Gillis, D., & Papadopoulos, A. (2023). "There was a lot of that [coercion and manipulation] happening and well, that's not very trustworthy": a qualitative study on COVID-19 vaccine hesitancy in Canada. Review of Communication, 23(3), 165–182. https://doi.org/10.1080/15358593.2022.2123251

Maloney, E. K., White, A. J., Samuel, L., Boehm, M., & Bleakley, A. (2024). COVID-19 coverage from six network and cable news sources in the United States: Representation of misinformation, correction, and portrayals of severity. Public Understanding of Science, 33(1), 58-72. https://doi-org.ezproxy.jyu.fi/10.1177/09636625231179588

Markov, Č., & Min, Y. (2022). Understanding the Public's Animosity Toward News Media: Cynicism and Distrust as Related but Distinct Negative Media Perceptions. Journalism & Mass Communication Quarterly, 99(4), 1099–1125. https://doi.org/10.1177/10776990211061764

Martínez-García, L., & Ferrer, I. (2023). Fact-Checking Journalism: A Palliative Against the COVID-19 Infodemic in Ibero-America. Journalism & Mass Communication Quarterly, 100(2), 264–285. https://doi.org/10.1177/10776990231164168

Marwick, A., & Lewis, R. (n.d.). Media Manipulation and Disinformation Online. New York: Data & Society Research Institute

Masip, P., Suau, J., & Ruiz-Caballero, C. (2020). Incidental Exposure to Non-Like-Minded News through Social Media: Opposing Voices in Echo-Chambers' News Feeds. Media and communication (Lisboa), 8(4), 53-62. https://doi.org/10.17645/mac.v8i4.3146

Mena, P., Barbe, D., & Chan-Olmsted, S. (2020). Misinformation on Instagram: The Impact of Trusted Endorsements on Message Credibility. Social Media + Society, 6(2). https://doi.org/10.1177/2056305120935102

Mensah, I. K., Khan, M. K., Liang, J., Zhu, N., Lin, L., & Mwakapesa, D. S. (2023). The moderating influence of perceived government information transparency on COVID-19 pandemic information adoption on social media systems. Frontiers in psychology, 14. https://doi.org/10.3389/fpsyg.2023.1172094

Miller, C. H., Ivanov, B., Sims, J., Compton, J., Harrison, K. J., Parker, K. A., Parker, J. L., & Averbeck, J. M. (2013). Boosting the Potency of Resistance: Combining the Motivational Forces of Inoculation and Psychological Reactance. Human Communication Research, 39(1), 127–155. https://doi.org/10.1111/j.1468-2958.2012.01438.x

Milyavskaya, M., Inzlicht, M., Hope, N., & Koestner, R. (2015). Saying "no" to temptation: Want-to motivation improves self-regulation by reducing temptation rather than by increasing self-control. Journal of Personality and Social Psychology, 109(4), 677. https://doi.org/10.1037/pspp0000045

Mims, C. A. (2017). How Facebook's master algorithm powers the social network. Wall Street Journal. https://www.wsj.com/articles/how-facebooks-master-algorithm-powers-the-social-network-1508673600

Mitchell, A., Gottfried, J., Barthel, M., & Sumida, N. (2018). Distinguishing between factual and opinion statements in the news. Pew Research Center's Journalism Project. Retrieved from: https://policycommons.net/artifacts/617278/distinguishing-between-factual-and-opinion-statements-in-the-news/1598050/ on 06 Feb 2024. CID: 20.500.12592/5mn6bx

Molina, R. G. (2023). Youth in the face of disinformation: A qualitative exploration of Mexican college students' attitudes, motivations, and abilities around false news. Communication & Society, 36(2), 97–113. https://doi.org/10.15581/003.36.2.97-113

Moody, G., Galletta, D., Walker, J., & Dunn, B. (2011). Which Phish Get Caught? An Exploratory Study of Individual Susceptibility to Phishing. European Journal of Information Systems, 26(6), 564–584. https://doi-org.ezproxy.jyu.fi/10.1057/s41303-017-0058-x

Moussa, M. B., Radwan, A. F, & Zaid, B.. (2022). Resilience to Covid-Misinformation Among Youth in a Paternalistic Context: The Case of the UAE. American Communication Journal, 24(1), 1–14.

Navarro, R., Larrañaga, E., Yubero, S., & Víllora, B. (2020). Psychological Correlates of Ghosting and Breadcrumbing Experiences: A Preliminary Study among Adults. International Journal of Environmental Research and Public Health, 17(3). https://doi.org/10.3390/ijerph17031116

Neyazi, T. A., Yi Kai Ng, A., Kuru, O., & Muhtadi, B. (2022). Who Gets Exposed to Political Misinformation in a Hybrid Media Environment? The Case of the 2019 Indonesian Election. Social media + society, 8(3). https://doi.org/10.1177/20563051221122792

Nickerson, R. S. (1998). Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. Review of General Psychology, 2(2), 175-220. https://doi-org.ezproxy.jyu.fi/10.1037/1089-2680.2.2.175

Nicoli, N., Louca, S., & Iosifidis, P. (2022). Social Media, News Media, and the Democratic Deficit: Can the Blockchain Make a Difference? TripleC (Cognition, Communication, Co-Operation): Open Access Journal for a Global Sustainable Information Society, 20(2), 163–178. https://doi.org/10.31269/triplec.v20i2.1322

Olan, F., Liu, S., Neaga, I., & Alkhuraiji, A. (2016). How knowledge sharing and business process contribute to organizational performance: Using the fsQCA approach. Journal of Business Research, 69(11), 5222–5227. https://doi.org/10.1016/j.jbusres.2016.04.116

Oxford English Dictionary. (2023c). Compromise (n.). In Oxford English Dictionary. Retrieved September 2023, from https://doi.org/10.1093/OED/6557463678.

Oxford English Dictionary. (2023a). Digital (n. & adj.). In Oxford English Dictionary. Retrieved December 2023, from https://doi.org/10.1093/OED/1297556308.

Oxford English Dictionary. (2023d). Exposure (n.). In Oxford English Dictionary. Retrieved September 2023, from https://doi.org/10.1093/OED/7353587158.

Oxford English Dictionary. (2023f). Inoculation (n.). In Oxford English Dictionary. Retrieved July 2023, from https://doi.org/10.1093/OED/3808408084.

Oxford English Dictionary. (2023b). Liability (n.). In Oxford English Dictionary. Retrieved September 2023, from https://doi.org/10.1093/OED/6643304306.

Oxford English Dictionary. (2023e). Risk (n.). In Oxford English Dictionary. Retrieved December 2023, from https://doi.org/10.1093/OED/2698784569.

Oxford English Dictionary. (2023h). Security (n.). In Oxford English Dictionary. Retrieved December 2023, from https://doi.org/10.1093/OED/1169723014.

Oxford English Dictionary. (2023g). Trust (n.). In Oxford English Dictionary. Retrieved December 2023, from https://doi.org/10.1093/OED/5777528687.

Oxford English Dictionary. (2024). Vulnerable (adj.). In Oxford English Dictionary. Retrieved January 2024, from https://doi.org/10.1093/OED/1136519195

Paisana, M., Pinto-Martinho, A., & Cardoso, G. (2020). Trust and fake news: Exploratory analysis of the impact of news literacy on the relationship with news content in Portugal. Communication & Society, 33(2), 105-117. https://doi.org/10.15581/003.33.2.105-117

Palmatier, R. W., Houston, M. B., & Hulland, J. (2018). Review articles: Purpose, process, and structure. Journal of the Academy of Marketing Science, 46(1), 1–5. https://doi.org/10.1007/s11747-017-0563-4

Pamment, J., Nothhaft, H., Agardh-Twetman, H., Fjällhed, A. (2018). Countering Information Influence Activities: The State of the Art. Department of Strategic Communication, Lund University. https://lup.lub.lu.se/record/825192b8-9274-4371-b33d-2b11baa5d5ae

Parasuraman, R., & Manzey, D. H. (2010). Complacency and bias in human use of automation: An attentional integration. Human Factors, 52(3), 381–410. https://doi.org/10.1177/0018720810376055

Paul A. David, “Clio and the Economics of QWERTY,” American Economic Review, LXXV (1985), 332–337; idem, “Understanding the Economics of QWERTY: The Necessity of History,” in William N. Parker (ed.), Economic History and the Modern Economist (Hoboken, 1986), 30–49; W. Brian Arthur, “Self-reinforcing Mechanisms in Economics,” in Philip W. Anderson, Kenneth J. Arrow, and David Pines (eds.), The Economy as an Evolving Complex System (Redwood City, 1988), 9–31; idem, “Competing Technologies and Lock-in by Historical Small Events,” Economic Journal, XCIX (1989), 116–131; Stan J. Liebowitz and Stephen E. Margolis, "Are Network Externalities a New Source of Market Failure?" Research in Law and Economics, XVII (1995), 1–22; idem, "Path Dependence, Lock-in, and History," Journal of Law, Economics, and Organization, XI (1995), 205–26; idem, "Policy and Path Dependence: From QWERTY to Windows 95," Regulation: The Cato Review of Business and Government, 18, no. 3 (1995), 33–41.

Pennycook, G., & Rand, D. G. (2019). Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. Cognition, 188, 39-50. https://doi.org/10.1016/j.cognition.2018.06.011

Persily, N., & Tucker, J. A. (2020). Social Media and Democracy: The State of the Field, Prospects for Reform. https://doi.org/10.1017/9781108890960

PhishLabs. (2022). Quarterly threat trends & intelligence report: February 2022. Retrieved from: https://www.phishlabs.com/

Poch-Butler, S. L., Moreno, A., & Gelado-Marcos, R. (2023). The WHO's communication strategies on social media during the early stage of the 2021 COVID vaccination campaign. Revista de Comunicación, 22(1), 377–395. https://doi.org/10.26441/rc22.1-2022-3102

Pyrhönen, N., & Bauvois, G. (2020). Conspiracies beyond Fake News. Produsing Reinformation on Presidential Elections in the Transnational Hybrid Media System. Sociological inquiry, 90(4), 705-731. https://doi.org/10.1111/soin.12339

Qahri-Saremi, H., & Turel, O. (2023). Situational Contingencies in Susceptibility of Social Media to Phishing: A Temptation and Restraint Model. Journal of Management Information Systems, 40(2), 503–540. https://doi.org/10.1080/07421222.2023.2196779

Rainear, A. M., & Lachlan, K. A. (2022). The station scientist: Examining the impact of race and sex of broadcast meteorologists on credibility, trust, and information retention. Frontiers in communication, 7. https://doi.org/10.3389/fcomm.2022.1052277

Ravn-Højgaard, S., Jóhannsdóttir, V., Karlsson, R., Olavson, R., & Skorini, H. í. (2021). Particularities of media systems in the West Nordic countries. Nordicom review, 42(2), 102-123. https://doi.org/10.2478/nor-2021-0020

Rhodes, S. C. (2021). Filter Bubbles, Echo Chambers, and Fake News: How Social Media Conditions Individuals to Be Less Critical of Political Misinformation. Political Communication, 39(1), 1–22. https://doi.org/10.1080/10584609.2021.1910887

Roozenbeek, J., & van der Linden, S. (2019). The fake news game: Actively inoculating against the risk of misinformation. Journal of Risk Research, 22(5), 570–580. https://doi.org/10.1080/13669877.2018.1443491

Sánchez, L., & Baselga, S. (2023). Protecting democracy from disinformation: Implications for a model of communication. Empedocles: European Journal for the Philosophy of Communication, 14(1), 5–20. https://doi.org/10.1386/ejpc_00050_1

Scanlon, A., & Lee, G. A. (2007). The Use of the Term Vulnerability in Acute Care: Why Does It Differ and What Does It Mean? The Australian Journal of Advanced Nursing, 24(3), 54–59. https://search.informit.org/doi/10.3316/ielapa.403019203147763

Schiavo, R., Eyal, G., Obregon, R., Quinn, S. C., Riess, H., & Boston-Fisher, N. (2022). The science of trust: future directions, research gaps, and implications for health and risk communication. Journal of Communication in Healthcare, 15(4), 245–259. https://doi.org/10.1080/17538068.2022.2121199

Shi, Z., Liu, X., & Srinivasan, K. (2022). Hype News Diffusion and Risk of Misinformation: The Oz Effect in Health Care. Journal of Marketing Research, 59(2), 327–352. https://doi.org/10.1177/00222437211044472

Shin, D., Kee, K. F., & Shin, E. Y. (2023). The Nudging Effect of Accuracy Alerts for Combating the Diffusion of Misinformation: Algorithmic News Sources, Trust in Algorithms, and Users' Discernment of Fake News. Journal of Broadcasting & Electronic Media, 67(2), 141–160. https://doi.org/10.1080/08838151.2023.2175830

Slavtcheva-Petkova, V. (2019). Fighting Putin and the Kremlin's grip in neo-authoritarian Russia: The experience of liberal journalists. Journalism, 20(11), 1530-1546. https://doi.org/10.1177/1464884917708061

Snijders, C. and Keren, G. (2001), "Do you trust? Whom do you trust? When do you trust?". Advances in Group Processes, 18, 129-160. https://doi.org/10.1016/S0882-6145(01)18006-9

Society of Professional Journalists. (2014). SPJ Code of Ethics. https://www.spj.org/ethicscode.asp

Splendore, S., & Curini, L. (2020). Proximity Between Citizens and Journalists as a Determinant of Trust in the Media. An Application to Italy. Journalism studies, 21(9), 1167-1185. https://doi.org/10.1080/1461670X.2020.1725601

Štětka, V., Mazák, J., & Vochocová, L. (2021). "Nobody Tells us what to Write about": The Disinformation Media Ecosystem and its Consumers in the Czech Republic. Javnost, 28(1), 90-109. https://doi.org/10.1080/13183222.2020.1841381

Stubenvoll, M., Heiss, R., & Matthes, J. (2021). Media Trust Under Threat: Antecedents and Consequences of Misinformation Perceptions on Social Media. International Journal of Communication, 15, 2765–2786.

Study.com. (2024) Retrieved from https://study.com/academy/lesson/disconfirmation-bias-definition-theory-example.html

Sun, Y., & Lu, F. (2023). How Misinformation and Rebuttals in Online Comments Affect People's Intention to Receive COVID-19 Vaccines: The Roles of Psychological Reactance and Misperceptions. Journalism & Mass Communication Quarterly, 100(1), 145–171. https://doi.org/10.1177/10776990221084606

Taber, C., & Lodge, M. (2006). Motivated skepticism in the evaluation of political beliefs. American Journal of Political Science, 50(3), 755–769. Retrieved from: http://www.jstor.org/stable/3694247

Tandoc, E. C., Hellmueller, L., & Vos, T. P. (2013). Mind the Gap. Journalism Practice, 7(5), 539–554. https://doi.org/10.1080/17512786.2012.726503

The High-Level Expert Group. (2018). A Multi-dimensional Approach to Disinformation: Report of the Independent High-Level Group on Fake News and Online Disinformation. Directorate-General for Communication, Networks, Content, and Technology. Retrieved from: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation

Tsfati, Y., Boomgaarden, H. G., Strömbäck, J., Vliegenthart, R., Damstra, A., & Lindgren, E. (2020). Causes and consequences of mainstream media dissemination of fake news: Literature review and synthesis. Annals of the International Communication Association, 44(2), 157–173. https://doi.org/10.1080/23808985.2020.1759443

Turel, O., & Qahri-Saremi, H. (2016). Problematic Use of Social Networking Sites: Antecedents and Consequence from a Dual-System Theory Perspective. Journal of Management Information Systems, 33(4), 1087–1116. https://doi.org/10.1080/07421222.2016.1267529

Van Duyn, E., & Collier, J. (2019). Priming and fake news: The effects of elite discourse on evaluations of news media. Mass Communication and Society, 22(1), 29–48. https://doi-org.ezproxy.jyu.fi/10.1080/15205436.2018.1511807

Wardle, C. (2019). First Draft‘s essential guide to understanding information disorder. UK: First Draft News. Retrieved from https://firstdraftnews.org/wp-content/uploads/2019/10/Information_Disorder_Digital_AW.pdf?x76701

Weeks, B. E., & Gil de Zúñiga, H. (2021). What’s Next? Six Observations for the Future of Political Misinformation Research. American Behavioral Scientist, 65(2), 277–289. https://doi.org/10.1177/0002764219878236

Williams, B. D., & Webb, G. R. (2021). Social vulnerability and disaster: Understanding the perspectives of practitioners. Disasters, 45(2), 278–295. https://doi.org/10.1111/disa.12422

Williams, B. A., & Delli Carpini, M. X. (2004). Monica and bill all the time and everywhere: The collapse of gatekeeping and agenda setting in the new media environment. American Behavioral Scientist, 47(9), 1208–1230. https://doi.org/10.1177/0002764203262344

World Economic Forum. (2024). Global Risks Report 2024. Retrieved from https://www.weforum.org/publications/global-risks-report-2024/

Wu, Y., Kuru, O., Campbell, S. W., & Baruh, L. (2023). Explaining Health Misinformation Belief through News, Social, and Alternative Health Media Use: The Moderating Roles of Need for Cognition and Faith in Intuition. Health Communication, 38(7), 1416–1429. https://doi.org/10.1080/10410236.2021.2010891

Yanchenko, K., Shestopalova, A., von Nordheim, G., & Kleinen-von Königslöw, K. (2023). "Repressed Opposition Media" or "Tools of Hybrid Warfare"? Negotiating the Boundaries of Legitimate Journalism in Ukraine Prior to

Russia's Full-Scale Invasion. The international journal of press/politics, 194016122311677. https://doi.org/10.1177/19401612231167791

Yudarwati, G. A., Putranto, I. A., & Delmo, K. M. (2022). Examining the Indonesian government's social media use for disaster risk communication. Asian Journal of Communication, 32(1), 1–20. https://doi.org/10.1080/01292986.2021.2007274

Zalmanson, L., Oestreicher-Singer, G., & Ecker, Y. (2022). The Role of Social Cues and Trust in Users' Private Information Disclosure. MIS Quarterly, 46(2), 1109–1133. https://doi.org/10.25300/MISQ/2022/16288

Zimmermann, F. Kohring, M. (2020). Mistrust, Disinforming News, and Vote Choice: A Panel Survey on the Origins and Consequences of Believing Disinformation in the 2017 German Parliamentary Election. Political communication, 37:215–237. https://doi.org/10.1080/10584609.2019.1686095

APPENDICES

APPENDIX 1. Systematic Literature Review Articles

Title	Author	PLink
(Digital) Campaigning in Dissonant Public Spheres.	Koc-Michalska, Karolina; Klinger, Ulrike; Bennett, Lance; Römmele, Andrea	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=164130480&site=ehost-live
Believing and Sharing Information by Fake Sources: An Experiment.	Bauer, Paul C.; Clemm von Hohenberg, Bernhard	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=154226959&site=ehost-live
Comparative analysis of the information security environment in Ukraine and Poland (survey of journalists and editors).	Katerynych, Petro	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=159704397&site=ehost-live
Deception as a Bridging Concept in the Study of Disinformation, Misinformation, and Misperceptions: Toward a Holistic Framework.	Chadwick, Andrew; Stanyer, James	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=156007016&site=ehost-live
Examining the Indonesian government's social media use for disaster risk communication.	Yudarwati, Gregoria A.; Putranto, Ignatius A.; Delmo, Kate M.	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=155436843&site=ehost-live
Explaining Health Misinformation Belief through News, Social, and Alternative Health Media Use: The Moderating Roles of Need for Cognition and Faith in Intuition.	Wu, Yuanyuan; Kuru, Ozan; Campbell, Scott W.; Baruh, Lemi	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=163915254&site=ehost-live
Fact-checking in Spain: Perception and trust.	Calvo, Dafne; Valera-Ordaz, Lidia; Requena i Mora, Marina; Llorca-Abad, Germán	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=160042918&site=ehost-live
Fact-Checking Journalism: A Palliative Against the COVID-19 Infodemic in Ibero-America.	Martínez-García, Luisa; Ferrer, Iliana	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=163741202&site=ehost-live
Filter Bubbles, Echo Chambers, and Fake News: How Social Media Conditions Individuals to Be Less Critical of Political Misinformation.	Rhodes, Samuel C.	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=155184362&site=ehost-live
Foregrounding digital realities at the locked down raced margins: a culture-centered case study in Aotearoa.	Elers, Phoebe; Jayan, Pooja; Dutta, Mohan J.	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=170041434&site=ehost-live
Government communication strategy and its reflection on media construction of pandemic: A structured analysis of COVID-19 in India.	BasuThakur, Priyam; De, Sangita	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=170041436&site=ehost-live

How Misinformation and Rebuttals in Online Comments Affect People's Intention to Receive COVID-19 Vaccines: The Roles of Psychological Reactance and Misperceptions.	Sun, Yanqing; Lu, Fangcao	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=161971327&site=ehost-live
"IMITATION (IN)SECURITY" AND THE POLYSEMY OF RUSSIAN DISINFORMATION: A CASE STUDY IN HOW IRA TROLLS TARGETED U.S. MILITARY VETERANS.	BEAN, HAMILTON; HARTNETT, STEPHEN J.; BANAEI-KASHANI, FARNOUSH; JAFARIAN, HAADI; KOUTSOUKOS, ALEX	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=158107433&site=ehost-live
MEDIA COVERAGE AND ITS DETERMINANTS IN THE CONTEXT OF THE COVID-19 PANDEMIC.	GÁLIK, Slavomír; TOLNAIOVÁ, Sabína GÁLIKOVÁ	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=157059329&site=ehost-live
Media Trust Under Threat: Antecedents and Consequences of Misinformation Perceptions on Social Media.	STUBENVOLL, MARLIS; HEISS, RAFFAEL; MATTHES, JÖRG	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=152907058&site=ehost-live
Misinformation Exposure and Acceptance: The Role of Information Seeking and Processing.	Hwang, Yoori; Jeong, Se-Hoon	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=161588010&site=ehost-live
News on fake news: Logics of media discourses on disinformation.	Farkas, Johan	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=161528270&site=ehost-live
Personalization, Echo Chambers, News Literacy, and Algorithmic Literacy: A Qualitative Study of AI-Powered News App Users.	Du, Ying Roselyn	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=164648551&site=ehost-live
Protecting Against Disinformation: Using Inoculation to Cultivate Reactance Towards Astroturf Attacks.	Boman, Courtney D.	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=163665958&site=ehost-live
Protecting democracy from disinformation: Implications for a model of communication.	Sánchez, Lydia; Villanueva Baselga, Sergio	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=169703720&site=ehost-live
Resilience to Covid-Misinformation Among Youth in a Paternalistic Context: The Case of the UAE.	MOUSSA, MOHAMED BEN; RADWAN, AHMED FAROUK; ZAID, BOUZINE	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=159155906&site=ehost-live
Social Media, News Media, and the Democratic Deficit: Can the Blockchain Make a Difference?	Nicoli, Nicholas; Louca, Soulla; Iosifidis, Petros	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=161735520&site=ehost-live
The Fake News Phenomenon in the Context of the Covid-19 Pandemic. The Perception of Romanian Students.	CRUCIAN, Narcis	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=169745429&site=ehost-live
The Nudging Effect of Accuracy Alerts for Combating the Diffusion of Misinformation: Algorithmic News Sources, Trust in Algorithms, and Users' Discernment of Fake News.	Shin, Donghee; Kee, Kerk F.; Shin, Emily Y.	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=163617833&site=ehost-live

The science of trust: future directions, research gaps, and implications for health and risk communication.	Schiavo, Renata; Eyal, Gil; Obregon, Rafael; Quinn, Sandra C.; Riess, Helen; Boston-Fisher, Nikita	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=160848737&site=ehost-live
The WHO's communication strategies on social media during the early stage of the 2021 COVID vaccination campaign.	Poch-Butler, S. L.; Moreno, A.; Gelado-Marcos, R.	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=162932816&site=ehost-live
"There was a lot of that [coercion and manipulation] happening and well, that's not very trustworthy": a qualitative study on COVID-19 vaccine hesitancy in Canada.	MacKay, Melissa; Thaivalappil, Abhinand; McWhirter, Jennifer E.; Gillis, Daniel; Papadopoulos, Andrew	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=170041429&site=ehost-live
Understanding the Effects of Personalized Recommender Systems on Political News Perceptions: A Comparison of Content-Based, Collaborative, and Editorial Choice-Based News Recommender System.	Liao, Mengqi	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=164648553&site=ehost-live
Understanding the Public's Animosity Toward News Media: Cynicism and Distrust as Related but Distinct Negative Media Perceptions.	Markov, Čedomir; Min, Young	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=160303463&site=ehost-live
Whom to trust? Media exposure patterns of citizens with perceptions of misinformation and disinformation related to the news media.	Hameleers, Michael; Brosius, Anna; de Vreese, Claes H	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=157070708&site=ehost-live
Youth in the face of disinformation: A qualitative exploration of Mexican college students' attitudes, motivations, and abilities around false news.	Molina, Rocío Galarza	https://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=162911927&site=ehost-live
Correcting E-Cigarette Misinformation on Social Media: Responses from UAE Nationals Who Smoke.	Li, Kang; Shin, Donghee	https://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=164648552&login.asp&site=ehost-live
CRISIS & EMERGENCY RISK COMMUNICATION: Six Principles for OSH Professionals.	Law, Matt	https://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=163479498&login.asp&site=ehost-live
Hype News Diffusion and Risk of Misinformation: The Oz Effect in Health Care.	Shi, Zijun; Liu, Xiao; Srinivasan, Kannan	https://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=155885238&login.asp&site=ehost-live
Role of fake news and misinformation in supply chain disruption: impact of technology competency as moderator.	Chatterjee, Sheshadri; Chaudhuri, Ranjan; Vrontis, Demetris	https://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=165046526&login.asp&site=ehost-live
Security Vulnerabilities of SGX and Countermeasures: A Survey.	SHUFAN FEI; ZHENG YAN; WENXIU DING; HAOMENG XIE	https://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=160618666&login.asp&site=ehost-live
Situational Contingencies in Susceptibility of Social Media to Phishing: A Temptation and Restraint Model.	Qahri-Saremi, Hamed; Turel, Ofir	https://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=164440452&login.asp&site=ehost-live

Social Cohesion: Mitigating Societal Risk in Case Studies of Digital Media in Hurricanes Harvey, Irma, and Maria.	Gongora-Svartzman, Gabriela; Ramirez-Marquez, Jose E.	https://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=158391961&login.asp&site=ehost-live
The Influence of Trustworthiness and Technology Acceptance Factors on the Usage of e-Government Services during COVID-19: A Case Study of Post COVID-19 Greece.	Balaskas, Stefanos; Panagiotarou, Aliki; Rigou, Maria	https://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=160941407&login.asp&site=ehost-live
THE ROLE OF SOCIAL CUES AND TRUST IN USERS' PRIVATE INFORMATION DISCLOSURE.	Zalmanson, Lior; Oestreicher-Singer, Gal; Ecker, Yael	https://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=157194652&login.asp&site=ehost-live
The Social Amplification of Risk Framework: A Normative Perspective on Trust?	Bearth, Angela; Siegrist, Michael	https://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=158081968&login.asp&site=ehost-live
Trust and fake news: Exploratory analysis of the impact of news literacy on the relationship with news content in Portugal	Paisana M.; Pinto-Martinho A.; Cardoso G.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083993738&doi=10.15581%2f003.33.2.105-117&partnerID=40&md5=9ccdd21e13f4cad3ac1e235ab3e81662
Proximity Between Citizens and Journalists as a Determinant of Trust in the Media. An Application to Italy	Splendore S.; Curini L.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85079376102&doi=10.1080%2f1461670X.2020.1725601&partnerID=40&md5=01c1efce5c1ed19d98435198c6ab6684
Particularities of media systems in the West Nordic countries	Ravn-Højgaard S.; Jóhannsdóttir V.; Karlsson R.; Olavson R.; Skorini H.Í.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85103851664&doi=10.2478%2fnor-2021-0020&partnerID=40&md5=598abb54dfd6b89500f67e1e2508ae0a
“Nobody Tells us what to Write about”: The Disinformation Media Ecosystem and its Consumers in the Czech Republic	Štětka V.; Mazák J.; Vochocová L.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85096438130&doi=10.1080%2f13183222.2020.1841381&partnerID=40&md5=454ac74c1f5d92c90bc5a8a209e22630
The station scientist: Examining the impact of race and sex of broadcast meteorologists on credibility, trust, and information retention	Rainear A.M.; Lachlan K.A.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85145311980&doi=10.3389%2ffcomm.2022.1052277&partnerID=40&md5=1ffd88f99be7fc6be92735e0423abda3
Agenda setting and the political economy of fear: How crime news influences voters’ beliefs	Graziano P.R.; Percoco M.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85033782845&doi=10.1177%2f0192512116656947&partnerID=40&md5=8c2f1318dcb0399f592195c4560eca35
Conspiracies beyond Fake News. Produsing Reinformation on Presidential Elections in the Transnational Hybrid Media System	Pyrhönen N.; Bauvois G.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85074800091&doi=10.1111%2fsoin.12339

		&partnerID=40&md5=d9e243499c763b4f7c813491998a9cf9
Fighting Putin and the Kremlin's grip in neo-authoritarian Russia: The experience of liberal journalists	Slavtcheva-Petkova V.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85058976169&doi=10.1177%2f1464884917708061&partnerID=40&md5=88069905c6aafbb33b4c768f1b50f841
"Repressed Opposition Media" or "Tools of Hybrid Warfare"? Negotiating the Boundaries of Legitimate Journalism in Ukraine Prior to Russia's Full-Scale Invasion	Yanchenko K.; Shestopalova A.; von Nordheim G.; Kleinen-von Königslöw K.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85152297409&doi=10.1177%2f19401612231167791&partnerID=40&md5=b08e96cf89c993632c2c530ce471e35e
Fake news and its impact on trust in the news. Using the portuguese case to establish lines of differentiation	Quintanilha T.L.; Da Silva M.T.; Lapa T.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85069803365&doi=10.15581%2f003.32.3.17-33&partnerID=40&md5=1e3f6959b3cb64e2353a5d570bd0b0f9
The moderating influence of perceived government information transparency on COVID-19 pandemic information adoption on social media systems	Mensah I.K.; Khan M.K.; Liang J.; Zhu N.; Lin L.-W.; Mwakapesa D.S.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85164479792&doi=10.3389%2ffpsyg.2023.1172094&partnerID=40&md5=e447ec92b6e279c5c8e9b2e12dedf033
Deception as a Bridging Concept in the Study of Disinformation, Misinformation, and Misperceptions: Toward a Holistic Framework	Chadwick A.; Stanyer J.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85140876141&doi=10.1093%2fct%2fqtab019&partnerID=40&md5=0e83688e78b058d8bed3420f6dea141e
Auditing Algorithmic Bias on Twitter	Bartley N.; Abeliuk A.; Ferrara E.; Lerman K.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85109035740&doi=10.1145%2f3447535.3462491&partnerID=40&md5=09159e85450467db566d9633b44af6f3
COVID-19 coverage from six network and cable news sources in the United States: Representation of misinformation, correction, and portrayals of severity	Maloney E.K.; White A.J.; Samuel L.; Boehm M.; Bleakley A.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85164339474&doi=10.1177%2f09636625231179588&partnerID=40&md5=50fe795e0c318b0e6e450e9d7416e3be
Transparency in Portuguese media: From the buzzword to the unsolved regulatory challenge	Baptista C.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85142822756&doi=10.15847%2fobsOBS16220221952&partnerID=40&md5=18d133fca9f2a987bda66711c7d142ea
Populist twitter posts in news stories: Statement recognition and the polarizing effects on candidate evaluation and anti-immigrant attitudes	Heiss R.; von Sikorski C.; Matthes J.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85060152079&doi=10.1080%2f17512786.

		2018.1564883&partnerID=40&md5=9b19f76a98e7bd8b1c23c4c0fb0a98b2
The “Infodemic” Infodemic: Toward a More Nuanced Understanding of Truth-Claims and the Need for (Not) Combatting Misinformation	Krause N.M.; Freiling I.; Scheufele D.A.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85132670436&doi=10.1177%2f00027162221086263&partnerID=40&md5=ff8e792a3acf8a370247f5fec8658f5a
Incidental exposure to non-like-minded news through social media: Opposing voices in echo-chambers’ news feeds	Masip P.; Suau J.; Ruiz-Caballero C.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85098065082&doi=10.17645%2fmac.v8i4.3146&partnerID=40&md5=5540e3b46366cc4c92b93d7e32e12376
Who Gets Exposed to Political Misinformation in a Hybrid Media Environment? The Case of the 2019 Indonesian Election	Neyazi T.A.; Yi Kai Ng A.; Kuru O.; Muhtadi B.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85138674402&doi=10.1177%2f20563051221122792&partnerID=40&md5=31a930a0dd8723859b75238c151ce00a
Populism and media policy failure	Freedman D.	https://www.scopus.com/inward/record.uri?eid=2-s2.0-85052496965&doi=10.1177%2f0267323118790156&partnerID=40&md5=1f4d89aca7198e7773b30bedfb131b41

APPENDIX 2. Systematic Literature Review Article Grouped by Key terms

Misinformation & Disinformation	
Believing and Sharing Information by Fake Sources: An Experiment.	Bauer, Paul C.; Clemm von Hohenberg, Bernhard
Fact-checking in Spain: Perception and trust.	Calvo, Dafne; Valera-Ordaz, Lidia; Requena i Mora, Marina; Llorca-Abad, Germán
Fact-Checking Journalism: A Palliative Against the COVID-19 Infodemic in Ibero-America.	Martínez-García, Luisa; Ferrer, Iliana
MEDIA COVERAGE AND ITS DETERMINANTS IN THE CONTEXT OF THE COVID-19 PANDEMIC.	GÁLIK, Slavomír; TOLNAIOVÁ, Sabína GÁLIKOVÁ
Media Trust Under Threat: Antecedents and Consequences of Misinformation Perceptions on Social Media.	STUBENVOLL, MARLIS; HEISS, RAFFAEL; MATTHES, JÖRG
News on fake news: Logics of media discourses on disinformation.	Farkas, Johan
Protecting Against Disinformation: Using Inoculation to Cultivate Reactance Towards Astroturf Attacks.	Boman, Courtney D.
Social Media, News Media, and the Democratic Deficit: Can the Blockchain Make a Difference?	Nicoli, Nicholas; Louca, Soulla; Iosifidis, Petros
The Fake News Phenomenon in the Context of the Covid-19 Pandemic. The Perception of Romanian Students.	CRUCIAN, Narcis
Whom to trust? Media exposure patterns of citizens with perceptions of misinformation and disinformation related to the news media.	Hameleers, Michael; Brosius, Anna; de Vreese, Claes H
Youth in the face of disinformation: A qualitative exploration of Mexican college students' attitudes, motivations, and abilities around false news.	Molina, Rocío Galarza

Hype News Diffusion and Risk of Misinformation: The Oz Effect in Health Care.	Shi, Zijun; Liu, Xiao; Srinivasan, Kannan
Fake news and its impact on trust in the news. Using the portuguese case to establish lines of differentiation	Quintanilha T.L.; Da Silva M.T.; Lapa T.
Deception as a Bridging Concept in the Study of Disinformation, Misinformation, and Misperceptions: Toward a Holistic Framework	Chadwick A.; Stanyer J.
COVID-19 coverage from six network and cable news sources in the United States: Representation of misinformation, correction, and portrayals of severity	Maloney E.K.; White A.J.; Samuel L.; Boehm M.; Bleakley A.
The "Infodemic" Infodemic: Toward a More Nuanced Understanding of Truth-Claims and the Need for (Not) Combatting Misinformation	Krause N.M.; Freiling I.; Scheufele D.A.
Who Gets Exposed to Political Misinformation in a Hybrid Media Environment? The Case of the 2019 Indonesian Election	Neyazi T.A.; Yi Kai Ng A.; Kuru O.; Muhtadi B.
"IMITATION (IN)SECURITY" AND THE POLYSEMY OF RUSSIAN DISINFORMATION: A CASE STUDY IN HOW IRA TROLLS TARGETED U.S. MILITARY VETERANS.	BEAN, HAMILTON; HARTNETT, STEPHEN J.; BANAEI-KASHANI, FARNOUSH; JAFARIAN, HAADI; KOUTSOUKOS, ALEX
Explaining Health Misinformation Belief through News, Social, and Alternative Health Media Use: The Moderating Roles of Need for Cognition and Faith in Intuition.	Wu, Yuanyuan; Kuru, Ozan; Campbell, Scott W.; Baruh, Lemi
Misinformation Exposure and Acceptance: The Role of Information Seeking and Processing.	Hwang, Yoori; Jeong, Se-Hoon
The Nudging Effect of Accuracy Alerts for Combating the Diffusion of Misinformation: Algorithmic News Sources, Trust in Algorithms, and Users' Discernment of Fake News.	Shin, Donghee; Kee, Kerk F.; Shin, Emily Y.
Correcting E-Cigarette Misinformation on Social Media: Responses from UAE Nationals Who Smoke.	Li, Kang; Shin, Donghee

Methods & Models in Research and Communication	
Filter Bubbles, Echo Chambers, and Fake News: How Social Media Conditions Individuals to Be Less Critical of Political Misinformation.	Rhodes, Samuel C.
Social Cohesion: Mitigating Societal Risk in Case Studies of Digital Media in Hurricanes Harvey, Irma, and Maria.	Gongora-Svartzman, Gabriela; Ramirez-Marquez, Jose E.
Particularities of media systems in the West Nordic countries	Ravn-Højgaard S.; Jóhannsdóttir V.; Karlsson R.; Olavson R.; Skorini H.Í.
"Repressed Opposition Media" or "Tools of Hybrid Warfare"? Negotiating the Boundaries of Legitimate Journalism in Ukraine Prior to Russia's Full-Scale Invasion	Yanchenko K.; Shestopalova A.; von Nordheim G.; Kleinen-von Königslöw K.
COVID-19 coverage from six network and cable news sources in the United States: Representation of misinformation, correction, and portrayals of severity	Maloney E.K.; White A.J.; Samuel L.; Boehm M.; Bleakley A.
The "Infodemic" Infodemic: Toward a More Nuanced Understanding of Truth-Claims and the Need for (Not) Combatting Misinformation	Krause N.M.; Freiling I.; Scheufele D.A.
Examining the Indonesian government's social media use for disaster risk communication.	Yudarwati, Gregoria A.; Putranto, Ignatius A.; Delmo, Kate M.
Government communication strategy and its reflection on media construction of pandemic: A structured analysis of COVID-19 in India.	BasuThakur, Priyam; De, Sangita
News on fake news: Logics of media discourses on disinformation.	Farkas, Johan
Protecting democracy from disinformation: Implications for a model of communication.	Sánchez, Lydia; Villanueva Baselga, Sergio
The science of trust: future directions, research gaps, and implications for health and risk communication.	Schiavo, Renata; Eyal, Gil; Obregon, Rafael; Quinn, Sandra C.; Riess, Helen; Boston-Fisher, Nikita

The WHO's communication strategies on social media during the early stage of the 2021 COVID vaccination campaign.	Poch-Butler, S. L.; Moreno, A.; Gelado-Marcos, R.
"There was a lot of that [coercion and manipulation] happening and well, that's not very trustworthy": a qualitative study on COVID-19 vaccine hesitancy in Canada.	MacKay, Melissa; Thaivalappil, Abhinand; McWhirter, Jennifer E.; Gillis, Daniel; Papadopoulos, Andrew
Social Cohesion: Mitigating Societal Risk in Case Studies of Digital Media in Hurricanes Harvey, Irma, and Maria.	Gongora-Svartzman, Gabriela; Ramirez-Marquez, Jose E.
The Influence of Trustworthiness and Technology Acceptance Factors on the Usage of e-Government Services during COVID-19: A Case Study of Post COVID-19 Greece.	Balaskas, Stefanos; Panagiotarou, Aliki; Rigou, Maria
The Social Amplification of Risk Framework: A Normative Perspective on Trust?	Bearth, Angela; Siegrist, Michael
The moderating influence of perceived government information transparency on COVID-19 pandemic information adoption on social media systems	Mensah I.K.; Khan M.K.; Liang J.; Zhu N.; Lin L.-W.; Mwakapesa D.S.
Explaining Health Misinformation Belief through News, Social, and Alternative Health Media Use: The Moderating Roles of Need for Cognition and Faith in Intuition.	Wu, Yuanyuan; Kuru, Ozan; Campbell, Scott W.; Baruh, Lemi
"IMITATION (IN)SECURITY" AND THE POLYSEMY OF RUSSIAN DISINFORMATION: A CASE STUDY IN HOW IRA TROLLS TARGETED U.S. MILITARY VETERANS.	BEAN, HAMILTON; HARTNETT, STEPHEN J.; BANAEI-KASHANI, FARNOUSH; JAFARIAN, HAADI; KOUTSOUKOS, ALEX
Misinformation Exposure and Acceptance: The Role of Information Seeking and Processing.	Hwang, Yoori; Jeong, Se-Hoon

Trust in Media and News:	
(Digital) Campaigning in Dissonant Public Spheres.	Koc-Michalska, Karolina; Klinger, Ulrike; Bennett, Lance; Römmele, Andrea
Believing and Sharing Information by Fake Sources: An Experiment.	Bauer, Paul C.; Clemm von Hohenberg, Bernhard
Fact-checking in Spain: Perception and trust.	Calvo, Dafne; Valera-Ordaz, Lidia; Requena i Mora, Marina; Llorca-Abad, Germán
Government communication strategy and its reflection on media construction of pandemic: A structured analysis of COVID-19 in India.	BasuThakur, Priyam; De, Sangita
MEDIA COVERAGE AND ITS DETERMINANTS IN THE CONTEXT OF THE COVID-19 PANDEMIC.	GÁLIK, Slavomír; TOLNAIOVÁ, Sabína GÁLIKOVÁ
Media Trust Under Threat: Antecedents and Consequences of Misinformation Perceptions on Social Media.	STUBENVOLL, MARLIS; HEISS, RAFFAEL; MATTHES, JÖRG
Protecting democracy from disinformation: Implications for a model of communication.	Sánchez, Lydia; Villanueva Baselga, Sergio
Social Media, News Media, and the Democratic Deficit: Can the Blockchain Make a Difference?	Nicoli, Nicholas; Louca, Soulla; Iosifidis, Petros
Understanding the Public's Animosity Toward News Media: Cynicism and Distrust as Related but Distinct Negative Media Perceptions.	Markov, Čedomir; Min, Young
Whom to trust? Media exposure patterns of citizens with perceptions of misinformation and disinformation related to the news media.	Hameleers, Michael; Brosius, Anna; de Vreese, Claes H
Proximity Between Citizens and Journalists as a Determinant of Trust in the Media. An Application to Italy	Splendore S.; Curini L.
Agenda setting and the political economy of fear: How crime news influences voters' beliefs	Graziano P.R.; Percoco M.
Fighting Putin and the Kremlin's grip in neo-authoritarian Russia: The experience of liberal journalists	Slavtcheva-Petkova V.

“Repressed Opposition Media” or “Tools of Hybrid Warfare”? Negotiating the Boundaries of Legitimate Journalism in Ukraine Prior to Russia's Full-Scale Invasion	Yanchenko K.; Shestopalova A.; von Nordheim G.; Kleinen-von Königslöw K.
Deception as a Bridging Concept in the Study of Disinformation, Misinformation, and Misperceptions: Toward a Holistic Framework	Chadwick A.; Stanyer J.
COVID-19 coverage from six network and cable news sources in the United States: Representation of misinformation, correction, and portrayals of severity	Maloney E.K.; White A.J.; Samuel L.; Boehm M.; Bleakley A.
Populist twitter posts in news stories: Statement recognition and the polarizing effects on candidate evaluation and anti-immigrant attitudes	Heiss R.; von Sikorski C.; Matthes J.
Populism and media policy failure	Freedman D.
The disinformation order: Disruptive communication and the decline of democratic institutions.	Bennett, W. L., & Livingston, S. (2018).
Mistrust, Disinforming News, and Vote Choice: A Panel Survey on the Origins and Consequences of Believing Disinformation in the 2017 German Parliamentary Election	Zimmermann, F. Kohring, M.
Fighting for truth? The role perceptions of Filipino journalists in an era of mis- and disinformation	Balod & Hameleers (2021)
The station scientist: Examining the impact of race and sex of broadcast meteorologists on credibility, trust, and information retention	Rainear A.M.; Lachlan K.A.
Hype News Diffusion and Risk of Misinformation: The Oz Effect in Health Care.	Shi, Zijun; Liu, Xiao; Srinivasan, Kannan
Personalization, Echo Chambers, News Literacy, and Algorithmic Literacy: A Qualitative Study of AI-Powered News App Users.	Du, Ying Roselyn
The Nudging Effect of Accuracy Alerts for Combating the Diffusion of Misinformation: Algorithmic News Sources, Trust in Algorithms, and Users' Discernment of Fake News.	Shin, Donghee; Kee, Kerk F.; Shin, Emily Y.
Understanding the Effects of Personalized Recommender Systems on Political News Perceptions: A Comparison of Content-Based, Collaborative, and Editorial Choice-Based News Recommender System.	Liao, Mengqi

Social Media and Networks	
(Digital) Campaigning in Dissonant Public Spheres.	Koc-Michalska, Karolina; Klinger, Ulrike; Bennett, Lance; Römmele, Andrea
Examining the Indonesian government's social media use for disaster risk communication.	Yudarwati, Gregoria A.; Putranto, Ignatius A.; Delmo, Kate M.
Media Trust Under Threat: Antecedents and Consequences of Misinformation Perceptions on Social Media.	STUBENVOLL, MARLIS; HEISS, RAFFAEL; MATTHES, JÖRG
Social Media, News Media, and the Democratic Deficit: Can the Blockchain Make a Difference?	Nicoli, Nicholas; Louca, Soulla; Iosifidis, Petros
The Fake News Phenomenon in the Context of the Covid-19 Pandemic. The Perception of Romanian Students.	CRUCIAN, Narcis
The WHO's communication strategies on social media during the early stage of the 2021 COVID vaccination campaign.	Poch-Butler, S. L.; Moreno, A.; Gelado-Marcos, R.
Youth in the face of disinformation: A qualitative exploration of Mexican college students' attitudes, motivations, and abilities around false news.	Molina, Rocío Galarza
Situational Contingencies in Susceptibility of Social Media to Phishing: A Temptation and Restraint Model.	Qahri-Saremi, Hamed; Turel, Ofir
The moderating influence of perceived government information transparency on COVID-19 pandemic information adoption on social media systems	Mensah I.K.; Khan M.K.; Liang J.; Zhu N.; Lin L.-W.; Mwakapesa D.S.

Populist twitter posts in news stories: Statement recognition and the polarizing effects on candidate evaluation and anti-immigrant attitudes	Heiss R.; von Sikorski C.; Matthes J.
Incidental exposure to non-like-minded news through social media: Opposing voices in echo-chambers' news feeds	Masip P.; Suau J.; Ruiz-Caballero C.
Who Gets Exposed to Political Misinformation in a Hybrid Media Environment? The Case of the 2019 Indonesian Election	Neyazi T.A.; Yi Kai Ng A.; Kuru O.; Muhtadi B.
Explaining Health Misinformation Belief through News, Social, and Alternative Health Media Use: The Moderating Roles of Need for Cognition and Faith in Intuition.	Wu, Yuanyuan; Kuru, Ozan; Campbell, Scott W.; Baruh, Lemi
Misinformation Exposure and Acceptance: The Role of Information Seeking and Processing.	Hwang, Yoori; Jeong, Se-Hoon
Personalization, Echo Chambers, News Literacy, and Algorithmic Literacy: A Qualitative Study of AI-Powered News App Users.	Du, Ying Roselyn
Understanding the Effects of Personalized Recommender Systems on Political News Perceptions: A Comparison of Content-Based, Collaborative, and Editorial Choice-Based News Recommender System.	Liao, Mengqi
Correcting E-Cigarette Misinformation on Social Media: Responses from UAE Nationals Who Smoke.	Li, Kang; Shin, Donghee

Political Dynamics and Communication:	
(Digital) Campaigning in Dissonant Public Spheres.	Koc-Michalska, Karolina; Klinger, Ulrike; Bennett, Lance; Römmele, Andrea
Believing and Sharing Information by Fake Sources: An Experiment.	Bauer, Paul C.; Clemm von Hohenberg, Bernhard
Examining the Indonesian government's social media use for disaster risk communication.	Yudarwati, Gregoria A.; Putranto, Ignatius A.; Delmo, Kate M.
News on fake news: Logics of media discourses on disinformation.	Farkas, Johan
Social Media, News Media, and the Democratic Deficit: Can the Blockchain Make a Difference?	Nicoli, Nicholas; Louca, Soulla; Iosifidis, Petros
Youth in the face of disinformation: A qualitative exploration of Mexican college students' attitudes, motivations, and abilities around false news.	Molina, Rocío Galarza
Proximity Between Citizens and Journalists as a Determinant of Trust in the Media. An Application to Italy	Splendore S.; Curini L.
Agenda setting and the political economy of fear: How crime news influences voters' beliefs	Graziano P.R.; Percoco M.
Populist twitter posts in news stories: Statement recognition and the polarizing effects on candidate evaluation and anti-immigrant attitudes	Heiss R.; von Sikorski C.; Matthes J.
Who Gets Exposed to Political Misinformation in a Hybrid Media Environment? The Case of the 2019 Indonesian Election	Neyazi T.A.; Yi Kai Ng A.; Kuru O.; Muhtadi B.
Populism and media policy failure	Freedman D.

Health Communication:	
Fact-Checking Journalism: A Palliative Against the COVID-19 Infodemic in Ibero-America.	Martínez-García, Luisa; Ferrer, Iliana
Foregrounding digital realities at the locked down raced margins: a culture-centered case study in Aotearoa.	Elers, Phoebe; Jayan, Pooja; Dutta, Mohan J.
Government communication strategy and its reflection on media construction of pandemic: A structured analysis of COVID-19 in India.	BasuThakur, Priyam; De, Sangita
How Misinformation and Rebuttals in Online Comments Affect People's Intention to Receive COVID-19 Vaccines: The Roles of Psychological Reactance and Misperceptions.	Sun, Yanqing; Lu, Fangcao

MEDIA COVERAGE AND ITS DETERMINANTS IN THE CONTEXT OF THE COVID-19 PANDEMIC.	GÁLIK, Slavomír; TOLNAIOVÁ, Sabína GÁLIKOVÁ
Resilience to Covid-Misinformation Among Youth in a Paternalistic Context: The Case of the UAE.	MOUSSA, MOHAMED BEN; RADWAN, AHMED FAROUK; ZAID, BOUZINE
The science of trust: future directions, research gaps, and implications for health and risk communication.	Schiavo, Renata; Eyal, Gil; Obregon, Rafael; Quinn, Sandra C.; Riess, Helen; Boston-Fisher, Nikita
The WHO's communication strategies on social media during the early stage of the 2021 COVID vaccination campaign.	Poch-Butler, S. L.; Moreno, A.; Gelado-Marcos, R.
"There was a lot of that [coercion and manipulation] happening and well, that's not very trustworthy": a qualitative study on COVID-19 vaccine hesitancy in Canada.	MacKay, Melissa; Thaivalappil, Abhinand; McWhirter, Jennifer E.; Gillis, Daniel; Papadopoulos, Andrew
Hype News Diffusion and Risk of Misinformation: The Oz Effect in Health Care.	Shi, Zijun; Liu, Xiao; Srinivasan, Kannan
The moderating influence of perceived government information transparency on COVID-19 pandemic information adoption on social media systems	Mensah I.K.; Khan M.K.; Liang J.; Zhu N.; Lin L.-W.; Mwakapesa D.S.
COVID-19 coverage from six network and cable news sources in the United States: Representation of misinformation, correction, and portrayals of severity	Maloney E.K.; White A.J.; Samuel L.; Boehm M.; Bleakley A.
Fact-checking in Spain: Perception and trust.	Calvo, Dafne; Valera-Ordaz, Lidia; Requena i Mora, Marina; Llorca-Abad, Germán

Behavioral Aspects	
Protecting Against Disinformation: Using Inoculation to Cultivate Reactance Towards Astroturf Attacks.	Boman, Courtney D.
Resilience to Covid-Misinformation Among Youth in a Paternalistic Context: The Case of the UAE.	MOUSSA, MOHAMED BEN; RADWAN, AHMED FAROUK; ZAID, BOUZINE
"There was a lot of that [coercion and manipulation] happening and well, that's not very trustworthy": a qualitative study on COVID-19 vaccine hesitancy in Canada.	MacKay, Melissa; Thaivalappil, Abhinand; McWhirter, Jennifer E.; Gillis, Daniel; Papadopoulos, Andrew
THE ROLE OF SOCIAL CUES AND TRUST IN USERS' PRIVATE INFORMATION DISCLOSURE.	Zalmanson, Lior; Oestreicher-Singer, Gal; Ecker, Yael
The Social Amplification of Risk Framework: A Normative Perspective on Trust?	Bearth, Angela; Siegrist, Michael
Trust and fake news: Exploratory analysis of the impact of news literacy on the relationship with news content in Portugal	Paisana M.; Pinto-Martinho A.; Cardoso G.
Media Coverage and Its Determinants in the Context of the Covid-19 Pandemic.	Gáliks, S., & Tolnaiová, S. G. (2022).
The station scientist: Examining the impact of race and sex of broadcast meteorologists on credibility, trust, and information retention	Rainear A.M.; Lachlan K.A.
Explaining Health Misinformation Belief through News, Social, and Alternative Health Media Use: The Moderating Roles of Need for Cognition and Faith in Intuition.	Wu, Yuanyuan; Kuru, Ozan; Campbell, Scott W.; Baruh, Lemi
"IMITATION (IN)SECURITY" AND THE POLYSEMY OF RUSSIAN DISINFORMATION: A CASE STUDY IN HOW IRA TROLLS TARGETED U.S. MILITARY VETERANS.	BEAN, HAMILTON; HARTNETT, STEPHEN J.; BANAEI-KASHANI, FARNOUSH; JAFARIAN, HAADI; KOUTSOUKOS, ALEX
Misinformation Exposure and Acceptance: The Role of Information Seeking and Processing.	Hwang, Yoori; Jeong, Se-Hoon
Protecting democracy from disinformation: Implications for a model of communication.	Sánchez, Lydia; Villanueva Baselga, Sergio
Situational Contingencies in Susceptibility of Social Media to Phishing: A Temptation and Restraint Model.	Qahri-Saremi, Hamed; Turel, Ofir

Country-Specific Studies:	
Resilience to Covid-Misinformation Among Youth in a Paternalistic Context: The Case of the UAE.	MOUSSA, MOHAMED BEN; RADWAN, AHMED FAROUK; ZAID, BOUZINE
Particularities of media systems in the West Nordic countries	Ravn-Højgaard S.; Jóhannsdóttir V.; Karlsson R.; Olavson R.; Skorini H.Í.
“Nobody Tells us what to Write about”: The Disinformation Media Ecosystem and its Consumers in the Czech Republic	Štětka V.; Mazák J.; Vochocová L.
Agenda setting and the political economy of fear: How crime news influences voters’ beliefs	Graziano P.R.; Percoco M.
“Repressed Opposition Media” or “Tools of Hybrid Warfare”? Negotiating the Boundaries of Legitimate Journalism in Ukraine Prior to Russia's Full-Scale Invasion	Yanchenko K.; Shestopalova A.; von Nordheim G.; Kleinen-von Königslöw K.
The moderating influence of perceived government information transparency on COVID-19 pandemic information adoption on social media systems	Mensah I.K.; Khan M.K.; Liang J.; Zhu N.; Lin L.-W.; Mwakapesa D.S.
Incidental exposure to non-like-minded news through social media: Opposing voices in echo-chambers’ news feeds	Masip P.; Suau J.; Ruiz-Caballero C.

Understanding Information Polarization:	
Filter Bubbles, Echo Chambers, and Fake News: How Social Media Conditions Individuals to Be Less Critical of Political Misinformation.	Rhodes, Samuel C.
Populist twitter posts in news stories: Statement recognition and the polarizing effects on candidate evaluation and anti-immigrant attitudes	Heiss R.; von Sikorski C.; Matthes J.
Incidental exposure to non-like-minded news through social media: Opposing voices in echo-chambers’ news feeds	Masip P.; Suau J.; Ruiz-Caballero C.
Protecting democracy from disinformation: Implications for a model of communication.	Sánchez, Lydia; Villanueva Baselga, Sergio
Auditing Algorithmic Bias on Twitter	Bartley N.; Abeliuk A.; Ferrara E.; Lerman K.

Information Management and Security:	
Comparative analysis of the information security environment in Ukraine and Poland (survey of journalists and editors).	Katerynych, Petro
THE ROLE OF SOCIAL CUES AND TRUST IN USERS' PRIVATE INFORMATION DISCLOSURE.	Zalmanson, Lior; Oestreicher-Singer, Gal; Ecker, Yael
***Attitude (Psychology) *Cognition *Intuition *Surveys *Misinformation**	Heiss R.; von Sikorski C.; Matthes J.
Transparency in Portuguese media: From the buzzword to the unsolved regulatory challenge.	Baptista, C. F. (2022).
Security Vulnerabilities of SGX and Countermeasures: A Survey.	SHUFAN FEI; ZHENG YAN; WENXIU DING; HAOMENG XIE
Misinformation Exposure and Acceptance: The Role of Information Seeking and Processing.	Hwang, Yoori; Jeong, Se-Hoon
The Nudging Effect of Accuracy Alerts for Combating the Diffusion of Misinformation: Algorithmic News Sources, Trust in Algorithms, and Users' Discernment of Fake News.	Shin, Donghee; Kee, Kerk F.; Shin, Emily Y.

Addressing Vulnerabilities and Building Resilience:	
The moderating influence of perceived government information transparency on COVID-19 pandemic information adoption on social media systems	Mensah I.K.; Khan M.K.; Liang J.; Zhu N.; Lin L.-W.; Mwakapesa D.S.

Protecting Against Disinformation: Using Inoculation to Cultivate Reactance Towards Astroturf Attacks.	Boman, Courtney D.
Resilience to Covid-Misinformation Among Youth in a Paternalistic Context: The Case of the UAE.	MOUSSA, MOHAMED BEN; RADWAN, AHMED FAROUK; ZAID, BOUZINE
Causes and consequences of mainstream media dissemination of fake news: Literature review and synthesis.	Tsfati, Y., Boomgaarden, H. G., Strömbäck, J., Vliegenthart, R., Damstra, A., & Lindgren, E. (2020).
Media Trust Under Threat: Antecedents and Consequences of Misinformation Perceptions on Social Media.	STUBENVOLL, MARLIS; HEISS, RAFFAEL; MATTHES, JÖRG
The station scientist: Examining the impact of race and sex of broadcast meteorologists on credibility, trust, and information retention	Rainear A.M.; Lachlan K.A.
Security Vulnerabilities of SGX and Countermeasures: A Survey.	SHUFAN FEI; ZHENG YAN; WENXIU DING; HAOMENG XIE
Correcting E-Cigarette Misinformation on Social Media: Responses from UAE Nationals Who Smoke.	Li, Kang; Shin, Donghee

Cybersecurity and Technology:	
Social Media, News Media, and the Democratic Deficit: Can the Blockchain Make a Difference?	Nicoli, Nicholas; Louca, Soulla; Iosifidis, Petros
Role of fake news and misinformation in supply chain disruption: impact of technology competency as moderator.	Chatterjee, Sheshadri; Chaudhuri, Ranjan; Vrontis, Demetris
Situational Contingencies in Susceptibility of Social Media to Phishing: A Temptation and Restraint Model.	Qahri-Saremi, Hamed; Turel, Ofir
Combating Information Attacks in the Age of the Internet: New Challenges for Cognitive Engineering.	Endsley, M. R.

NO KEYTERMS	
CRISIS & EMERGENCY RISK COMMUNICATION: Six Principles for OSH Professionals.	Law, Matt
Conspiracies beyond Fake News. Produsing Reinformation on Presidential Elections in the Transnational Hybrid Media System	Pyrhönen N.; Bauvois G.