EDICIONES COMPLUTENSE

Estudios sobre el **Mensaje Periodístico**
ISSN-e: 1988-2696

ARTÍCULOS

Connecting Disinformation and Cybersecurity: An Interview-Based Exploration of Practice and Research Perspectives

Teresa García-Alcaraz
Universidad de Murcia
Juan Miguel Aguado-Terrón
Universidad de Murcia
José A. Ruipérez-Valiente
Universidad de Murcia

https://dx.doi.org/10.5209/esmp.106906 Received: January 8, 2026 • Accepted: May 20, 2026

ENG **Abstract.** This study examines how experts conceptualize the relationship between disinformation and cybersecurity and how these perceptions evolve when confronted with concrete cases and mechanisms. Building on recent efforts to frame disinformation within security and cyber intelligence approaches, we conduct semi-structured expert interviews to capture multidisciplinary viewpoints on an emerging and conceptually fragmented field. Eight informants —equally split between professional and academic domains— include fact-checkers, journalists, military and policy practitioners, and scholars in communication, law, propaganda studies, and cybersecurity. The interview protocol explores perceptions of the disinformation-cybersecurity link, its nature and proximity, campaigns with potential national security implications, disinformation wars, the role of artificial intelligence, overlaps between cybercrime and disinformation actors, and mitigation strategies. Findings indicate broad agreement that a link exists but divergence in how it is defined: most participants initially describe it as circumstantial, whereas security-oriented profiles more often treat it as structural and direct. As interviews progress, positions tend to converge and latent connections surface, revealing disciplinary biases and occasional inconsistencies, particularly among those equating cybersecurity primarily with cybercrime or foregrounding freedom-of-expression risks. Across profiles, AI is widely viewed as accelerating targeting and dissemination, while also enabling improved detection and assessment. Proposed responses emphasize education and resilience-building, detection, and institutional measures, underscoring the need for shared concepts and interdisciplinarity to support coherent analysis and mitigation of disinformation as a cybersecurity-relevant threat.
Keywords: Disinformation, cybersecurity, expert interviews, national security, artificial intelligence.

ES Conectando desinformación y ciberseguridad: un análisis exploratorio basado en entrevistas con perfiles profesionales y académicos

Resumen. Esta investigación analiza cómo diferentes expertos entienden la relación entre la desinformación y la ciberseguridad, así como esas percepciones cambian cuando se discuten casos y mecanismos concretos. A partir de los intentos recientes por situar la desinformación dentro de enfoques de ciberseguridad, se realizaron entrevistas semiestructuradas a fin de recoger miradas multidisciplinares en un ámbito emergente y aún poco consolidado conceptualmente. La muestra estuvo compuesta por ocho perfiles profesionales y académicos. El guion indagó si se percibe un vínculo entre desinformación y ciberseguridad y cómo se define su naturaleza y su cercanía; además, se recopilaron campañas con posibles implicaciones para la seguridad nacional, se exploró el concepto de «guerras de desinformación», se evaluó el papel de la IA, se examinó el solapamiento percibido entre actores del cibercrimen y de la desinformación, y se recogieron propuestas de mitigación. Los resultados muestran un acuerdo general en que existe relación, aunque con desacuerdos, sobre cómo caracterizarla. Conforme avanza la entrevista, las posturas suelen acercarse y afloran conexiones menos evidentes, poniendo de relieve sesgos disciplinares e inconsistencias puntuales, especialmente cuando se asimila la ciberseguridad casi exclusivamente al cibercrimen o se priorizan los riesgos para la libertad de expresión. En conjunto, la IA se percibe como un acelerador, pero también como apoyo para mejorar la detección y la evaluación. Las respuestas propuestas se centran en educación y construcción de resiliencia, detección y medidas institucionales, lo que refuerza la necesidad de conceptos compartidos e interdisciplinariedad para analizar y mitigar la desinformación.
Palabras clave: Desinformación, ciberseguridad, entrevista a expertos, seguridad nacional, inteligencia artificial.

How to cite: García-Alcaraz, T., Aguado-Terrón, J.M., & Ruipérez-Valiente, J.A. (2026). Connecting Disinformation and Cybersecurity: An Interview-Based Exploration of Practice and Research Perspectives. *Estudios sobre el Mensaje Periodístico*, *32*(3), 529-543. https://dx.doi.org/10.5209/esmp.106906

1. Introduction

Disinformation has evolved into a complex and multifaceted phenomenon that poses a significant threat to the political and social structures of contemporary societies. It has been defined as a dangerous form of information disorder (Wardle & Derakhshan, 2017), characterized by intentionality (Arsenault, 2020). This intentionality is expressed through strategic attacks aimed at altering the ideological and informational environment in which citizens operate, via the systematic dissemination of lies, conspiracies and rumors (Vasu *et al.*, 2018).

Far from being an isolated or sporadic phenomenon, disinformation constitutes a systematic strategy with multiple objectives, seeking to undermine and distort the truth (Bennett & Livingston, 2018). Aguado and Gómez de Ágreda (2023) broaden this perspective by arguing that disinformation involves a wide spectrum of actors, including not only state entities and traditional media but also companies, political parties, organized social movements and a growing industry of intermediaries that facilitate the technical, logistical and scaling dimensions of disinformation campaigns (Rodríguez-Fernández & Establés, 2023).

Despite the proliferation of academic work on disinformation, much of the literature still focuses primarily on the nature of messages and their socio-political effects, framing disinformation mainly as a 'media problem' (Arsenault, 2020; Bechmann, 2020; Kapantai *et al.*, 2021). This fragmented view contrasts with the increasing complexity of cyberspace, where disinformation is ever more tightly intertwined with different dimensions of the social sphere and has become a crucial component of cybersecurity (Aguado and Gómez de Ágreda, 2023).

In parallel, since 2019, several initiatives have sought to apply or adapt cybersecurity frameworks to the analysis, identification, and prevention of disinformation campaigns. Among them, the MITRE ATT&CK framework (2025) has been partially adapted to address informational threats. In contrast, the DISARM project (DISARM Foundation, 2024) was conceived from the outset to model tactics, techniques, and procedures (TTPs) of influence operations. However, Kapantai *et al.* (2021) warn of the risk that such technical and computational frameworks, together with algorithmic solutions for fake news detection, may inadvertently frame disinformation as a national security threat and focus almost exclusively on efficiency, without fully acknowledging it as a complex process embedded in a specific ecosystem.

At the same time, the impact of disinformation on public opinion has led governments and international organizations, such as the European Union, to establish joint mechanisms to combat this information disorder (Bechmann, 2020; Cea *et al.*, 2023; López *et al.*, 2025). The World Economic Forum (2024) highlights in its Global Risks Report that cybersecurity and disinformation rank among the principal risk factors for the next two years. Nevertheless, as Bechmann (2020) notes, many of the strategies implemented continue to prioritize content, while neglecting the broader context in which disinformation and infodemics develop, which results in measures that do not adequately address underlying problems in media and communication infrastructures.

The growing interest in approaching disinformation as a security issue is also evident in recent NATO documents (NATO Strategic Communications Centre of Excellence, 2025), which describe information manipulation by foreign actors as a real threat capable of polarizing societies, eroding public trust and weakening fundamental democratic institutions.

Against this backdrop, the recent assimilation of disinformation as a threat to national security necessarily links disinformation phenomena to the field of cybersecurity (Caramancion, 2020). Taking into account its social complexity, the diversity of actors and processes involved, and the pervasiveness of digital technology as an escalating factor, recognizing and categorizing disinformation as a cybersecurity threat would allow for a more precise analysis of its nature and the development of appropriate mitigation strategies.

However, significant conceptual and disciplinary gaps persist. Much work remains to be done to reach a minimum consensus across fields on basic reference points such as categorization criteria or definitions of disinformation types (Kapantai *et al.*, 2021). The primary objective of this research is to assess how professional and academic profiles relate to different perceptions of the link between disinformation and cybersecurity, understanding how high-level experts articulate these connections. Following Mirza *et al.* (2023), expert in-depth interviews are employed to approach this relatively new field from a multidisciplinary and open perspective. Sample profiling follows criteria of specialization (research, training, and/or management responsibilities in disinformation and cybersecurity) and availability.

1.1. Research objectives

Within this framework, a preliminary exploratory study is proposed, guided by the following objectives:

O1. Examine how disinformation and cybersecurity are conceptualised in academic and professional domains and explore how these conceptions relate.

O2. Identify less evident connections between both fields in order to assess whether and how expert perceptions shift when confronted with concrete cases and examples.

O3. Detect and highlight analytical gaps across different knowledge domains involved in studying and addressing disinformation and cybersecurity.

1.2. Contributions and novelty

Given the increasing social and political relevance of disinformation as a transformative phenomenon within the informational ecosystem (Kapantai *et al.*, 2021), this study offers a transdisciplinary framework that brings together diverse academic and professional perspectives surrounding the challenges posed by the nexus of disinformation and cybersecurity.

By exploring the complex connections between cyberthreats and information manipulation, this work emphasizes frequently overlooked dimensions of disinformation that extend beyond media-centered interpretations. In doing so, it seeks to open new conceptual and analytical avenues and contribute to the development of more comprehensive and effective strategies to address this emerging threat.

2. Methodology

The study employed semi-structured expert in-depth interviews, following Mirza *et al.* (2023), to capture multidisciplinary perspectives on this emerging field. The use of expert interviews is particularly suitable for exploring complex and multidisciplinary fields in which knowledge is distributed across institutional, professional, and academic actors (Ben Aharon, 2023; Von Soest, 2023). This is especially relevant in the study of disinformation, a field that remains highly fragmented across disciplines and still dominated by data-driven approaches, which makes qualitative contributions especially valuable (Broda & Strömbäck, 2024). The sample was constructed according to criteria of specialization (including research, training, and/or management responsibilities in disinformation and cybersecurity) and availability, ensuring representation from both professional and academic domains. After defining the expertise areas for the profiles that would make up our sample, we selected candidates for each profile based on their availability.

Profiles from the professional sphere included fact-checkers, journalists and military personnel with expertise in disinformation, while profiles from the academic sphere included researchers in law, propaganda and cybersecurity. The final panel comprised eight expert profiles, evenly split between professional and academic domains. All informants possessed highly specialized knowledge of disinformation phenomena.

To guarantee anonymity, participants' names have been removed, and professional or academic profiles are used as codes in order to contextualize and categorize the answers efficiently. No formal ethics committee approval was required under the institutional procedures applicable to this study. Participation was voluntary and based on informed consent, which was obtained in writing from all interviewees. Interviewees were informed of the academic purpose of the study and of the anonymized treatment of their responses. Given the sensitivity of some profiles, particularly those linked to defense and public administration, identifying details were minimized, and interview materials were stored securely and used exclusively for research purposes.

Table 1. Summarizes the professional and academic profiles of the informants.

Profile	Institutional field / sector	Core disciplinary background	Main role re: disinformation	Type of expertise	Disinformation-cybersecurity nexus	Dominant perspective on disinformation
Professional profile 1	Armed forces and defense (Air Force, Joint Cyberspace Command, NATO CoE)	Industrial engineering; defense & security policy; terrorism and counter-terrorism studies	Cyber defense strategist and practitioner; expert on cognitive / information operations	Hybrid: Operational + Policy + Academic	Cognitive ecosystem, information operations and cyber defense	Security-defense, multidisciplinary and systemic
Professional profile 2	OSINT, digital investigation and verification	Open Source Intelligence, verification and investigative practice	OSINT / verification specialist fighting disinformation and documenting war crimes	Operational / Practitioner	OSINT-based detection, verification and legal accountability around disinformation	Accountability and evidence (OSINT / investigation)
Professional profile 3	Journalism and media	Journalism and communication	Street correspondent and columnist using social media; covers disinformation issues	Communication / Dissemination + Practitioner	News production, social networks and disinformation coverage	Media-journalism and social media
Professional profile 4	National security and cyber policy	Business administration; information security management; defense studies	National security and cybersecurity advisor; member of cybersecurity and disinformation fora	Policy / Strategic + Practitioner	National security, cyber policy and institutional response to disinformation	Policy-governance, national security
Academic profile 1	University (communication, corporate communication and propaganda)	Information science; corporate communication; propaganda studies	University lecturer and researcher on propaganda and digital media	Academic / Research	Digital propaganda and its relationship with disinformation	Propaganda-strategic communication

Profile	Institutional field / sector	Core disciplinary background	Main role re: disinformation	Type of expertise	Disinformation-cybersecurity nexus	Dominant perspective on disinformation
Academic profile 2	University (law / administrative law)	Law (administrative law); innovation, law and technology	Legal scholar teaching cybersecurity and disinformation in master's programs	Academic / Research	Legal and regulatory frameworks for cybersecurity and disinformation	Legal-institutional and governance
Academic profile 3	University (educational technologies and cyber defense)	Educational technologies; human-computer interaction; data science; cyber defense	Full-time researcher on educational technologies, data and cyber defense; participant in EU defense-disinformation project	Academic / Research (technical)	Data- and HCI-driven analysis of disinformation in defense and military contexts	Socio-technical / data-HCI and cyber defense
Academic profile 4	Cybersecurity outreach and public communication	Journalism and communication	Journalist leading an information project on cybersecurity and digital awareness	Communication / Dissemination	Public communication on cybersecurity, digital awareness and disinformation	Public engagement and awareness-raising

Source: Own formulation.

Following methodological guidelines on expert interviews (De Miguel, 2005; Palacios & Rubio, 2003), in-depth interviews involved nine semi- structured questions designed to encourage complex responses in a fluid conversational environment. The interviews were conducted via video call during January 2025, each lasting between 45 minutes and 1 hour.

The structure of the questionnaire combined positioning questions with identification of cases and examples, and control and prospective questions related to different aspects of the relationship between disinformation and cybersecurity. Questions are divided into six thematic categories:

The first category (Q1) addresses participants' perceptions on the association between the field of disinformation and that of cybersecurity. For analytical purposes, the researchers established a priori two coding dimensions for this block—nature (structural/circumstantial) and proximity (direct/indirect). These categories were not presented to participants as closed response options; rather, interviewees were invited to reflect openly on the existence and characteristics of the possible link, and their responses were subsequently classified according to these analytical dimensions. In the second category, Q2 and Q3 ask participants to identify disinformation campaigns that have impacted national security and addressing the perceived impact of these campaigns.

The third category (Q4, Q5) focuses on national security, introducing the term 'disinformation wars', to demand positioning and perspective about its possible descriptive validity, and (if consistent) the levels and scale they attribute to it in identified cases. Q5 focuses on the perceived effects of disinformation attacks as a control question addressed to check disinformation security implications.

In the fourth section (Q6), specific insights are demanded about the role of artificial intelligence in disinformation campaigns and whether the involvement of AI in the (dis)information environment urges to consider disinformation as a type of cyber threat (Kertysova, 2018; Khan, 2025; Mazurczyk *et al.*, 2024).

Fifth category (Q7, Q8) adopts a different approach to the link between disinformation and cybersecurity, examining possible perceived connections between actors in cybercrime and disinformation environments and how potential advancements in one field might foster developments in the other.

Finally, sixth category (Q9) addresses prospective insights on actions, policies, or strategies to combat disinformation.

Table 2. Summarizes the questions and their categorization in the interview strategy.

Q	Thematic category	Main focus / analytical angle	Key concepts
Q1	Category 1 - Perception of the link between disinformation-cybersecurity	Captures whether respondents see a relationship between disinformation and cybersecurity, and how they characterize it (e.g. structural vs. circumstantial; direct vs. indirect).	Nature (structural/ circumstantial), Proximity (direct/ indirect)
Q2	Category 2 - Cases impacting national security	Elicits concrete examples of disinformation campaigns with (potential) national security implications, useful for case mapping and empirical grounding.	Identification of cases, Impact assessment
Q3	Category 2 - Cases and perceived impact	Assesses perceived adequacy of current recognition of disinformation's impact in Spain (policies, strategies, public discourse).	Policies,Strategies, Public discourse
Q4	Category 3 - 'Disinformation wars' and scale	Explores whether respondents accept the notion of 'disinformation wars', at which levels and scales, and with which illustrative cases.	Levels, Extent, Relevant cases
Q5	Category 3 - Effects on security (control question)	Identifies perceived harmful effects of disinformation (institutions, social cohesion, critical infrastructure, military operations, etc.) as a control for security implications.	Most pernicious effects, Security implications
Q6	Category 4 - AI, disinformation and cyber threats	Gathers views on how AI reshapes disinformation campaigns and whether this reinforces treating disinformation as a cyber threat.	AI involvement, Cyber threat consideration
Q7	Category 5 - Actors and ecosystems	Probes perceived overlaps or coordination between cyberattack/cybercrime actors and disinformation actors (shared infrastructures, incentives, environments).	Actor connections, Environment similarities
Q8	Category 5 - Mutual influence between fields	Examines whether respondents see synergies or feedback loops between advances in cybersecurity and advances in counter-disinformation.	Improvements, Impact assessment
Q9	Category 6 - Prospective strategies and policy	Collects proposed measures (policies, strategies, operational responses) to counter disinformation, allowing later classification by level and type.	Policy measures, Operational responses, Governance levels

Source: Own formulation.

The analysis followed a qualitative thematic procedure. First, responses were organized according to the six thematic categories defined in the interview guide. Second, the material was compared across profiles in order to identify recurring patterns, divergences, and discursive inconsistencies in how the relationship between disinformation and cybersecurity was understood. To enhance credibility and traceability, the interpretation was grounded in the original interview structure, the systematic use of profile-based coding, and the progressive organization of results into comparative tables and thematic blocks, which made it possible to track how each analytical conclusion related to specific questions and profile types.

3. Findings and discussion

The material gathered in these interviews provides an overview of how disinformation is understood from different academic and professional profiles, particularly if this is conceived as a media-exclusive social phenomenon or whether it is understood to have wider social implications. It also allows us to address the differences between profiles, possible biases and unintentional inconsistencies in discourse. The findings and subsequent discussions have been categorized into thematic blocks to facilitate comprehension.

3.1. The link between disinformation and cybersecurity and its characteristics

In this preliminary block, participants were asked to consider the existence of any potential connection between disinformation and cybersecurity, as well as the characteristics of such a link, if applicable. For analytical purposes, their open-ended responses were later classified according to the categories of nature (structural/circumstantial) and proximity (direct/indirect).Q1 is designed to reveal the explicit or manifest thinking of the interviewees. Table 3 summarizes the results for Q1, including the responses to the question of whether the consideration of disinformation in Spain was adequate to its potential impact (Q3). Considering together responses to Q1 and Q3 will help in understanding further implications in block 2.

Table 3. Recognition or not of the link between disinformation and cybersecurity, and its characteristics.

Profile	Sphere	Identifies link between disinformation and cybersecurity	Type	Proximity	Consideration of disinformation in Spain
Professional profile 1	Defense/ cyberdefense	Yes	Structural	Direct	Yes
Professional profile 2	OSINT and verification	Yes	Circumstantial	Indirect	Yes
Professional profile 3	Journalist	Yes	Circumstantial	Direct	No
Professional profile 4	Public administrations	Yes	Circumstantial	Indirect	No
Academic profile 1	Propaganda	Yes	Circumstantial	Direct	No
Academic profile 2	Law	Yes	Circumstantial	Indirect	Yes
Academic profile 3	Cybersecurity and data science	Yes	Structural	Direct	No
Academic profile 4	Dissemination	Yes	Circumstantial	Direct	No

Source: Own formulation.

Note: N = 8. Percentages reported in the text are calculated over the full panel of interviewees. The categories "type" (structural/ circumstantial) and "proximity" (direct/indirect) were established by the researchers as analytical coding dimensions for Q1 and applied to participants' open-ended responses. The final column incorporates the open-ended assessment corresponding to Q3 ("consideration of disinformation in Spain").

While all interviewees concur with the notion that there is a connection between disinformation and cybersecurity, divergent perspectives emerge upon further probing, particularly concerning the nature of this connection. The spectrum of perceptions can be summarized into two main categories for the kind of connection between disinformation and cybersecurity: structural versus circumstantial.

'Structural' refers to an inherent connection in the system's foundations, stemming from the essential characteristics of both phenomena. This is considered a profound, inevitable connection. Conversely, interviewees characterize the relationship between disinformation and cybersecurity as circumstantial when they recognize that this association originates from particular, short-term, or context-dependent circumstances.

75% of interviewees are of the opinion that the correlation between disinformation and cybersecurity is circumstantial, mainly because both phenomena occur within the cyber environment.

In this regard, no distinctions are observed between the academic and professional profiles. Disparities emerge from the specific professional field or academic domain in which the interviewees operate (and their specializations). The two interviewees who do think that the relationship between both phenomena is structural are those dedicated to national security and cybersecurity, one from a professional profile and the other from an academic profile.

On the other hand, the category of proximity refers to the degree to which these relationships are interconnected, with direct proximity occurring when one element's characteristics immediately impact another. For instance, "greater investment in cybersecurity leads to less disinformation". In contrast, proximity is deemed indirect when respondents view the relationship as mediated by an intermediary factor or occurring only sporadically.

This question generates more discrepancies among interviewees. The two interviewees who answered that the relationship between disinformation and cybersecurity is structural also indicate, consequently, that it is direct.

37.5% of interviewees think that the proximity between disinformation and cybersecurity is indirect, arguing that this relationship only occurs through intermediary factors such as psychology, anthropology, sociology, or, in the case of the academic profile sharing this view, from the legal field. They all share the assumption that this relationship simply occurs because of the ambiguity or vagueness of both terms.

One of the relevant pitfalls in building a consensus is the dimensional difference between disinformation and cybersecurity in terms of gravity and scale of effects. As one of the informants puts it, "a cyberattack always implies crime or attempted crime and is, in my view, a much more serious level on the scale of problems. Disinformation corresponds to broader factors, and sometimes it is not even intentional" (the informant's profile, relevantly, is that of a professional with expertise in OSINT and verification). As far as the concept of cybersecurity implies cybercrime, interviewees appear reluctant to establish a link between disinformation and cybercrime. Particularly because cybercrime is seen to be a 'hard' social category (in terms of its nature and effects), while disinformation is understood as a 'soft ' category due to its vagueness.

3.2. Identifying disinformation campaigns having impact on national security and consistency with the consideration of disinformation in Spain

In Q2 and Q3, the inquiry was directed towards the awareness of disinformation campaigns that have had or could have an impact on national security. This is an indirect way to consider the implicit connection between disinformation and cybersecurity by ap-

proaching the potential threat that disinformation poses to a nation's security. There is, in fact, a growing corpus of literature in this field, which allows to presume a high level of consensus between interviewees.

The 2019 Annual Report on National Security in Spain (Department of National Security, 2020) was the first to highlight disinformation as a significant problem within the framework of Spanish national security, establishing a precedent that subsequent reports have consistently reiterated. The most recent Homeland Security report (Department of National Security, 2025) identifies disinformation as the primary threat to Spain for the first time in the risk perception survey, with the vulnerability of cyberspace ranking as the second most significant risk.

The appearance of these two types of risk together is not circumstantial, as the report emphasizes. Some characteristics pointed out in that document include that both converge in the same medium (the cybernetic), both are identified as risks closely related to electoral processes, and both are carried out by foreign actors that may or may not be state actors.

Accordingly, informants concurr that one of the most significant relationships between disinformation and the field of cybersecurity is that both occur in cyberspace. One might inquire whether the fact that disinformation is a type of national security risk that takes place in cyberspace is necessarily synonymous with a type of cyber-risk or cyberthreat, which necessarily links it to the field of cybersecurity.

Addressing Q2, the fact that all interviewees state and list cases in which disinformation campaigns have posed a danger to national security indicates that they identify it as such, at least implicitly. This poses a clear contradiction with those views considering the nature of the relationship between disinformation and cybersecurity as circumstantial.

The cases cited by each interviewee have been categorized into six classifications based on the value vectors in disinformation ecosystems identified by Aguado and Gómez de Ágreda (2023). These categories have been arranged in descending order according to the number of times each case was cited. The categories are as follows:

1. Political influence (87.5%): seven interviewees cited cases related to electoral interference or the influence of public debate.
2. Disruption of affective networks (50%): half of the interviewees cite cases of narratives leading to hyper-individualism and denialism or impacting beliefs in general. Two interviewees relate this type of effect to campaigns that took place during the pandemic involving loss of human lives.
3. Undermining institutions (37.5%): questioning the nation-system, its leaders or society´s perception of a war (domestic or foreign). This category is mentioned by three out of eight interviewees.
4. Undermining social cohesion (25%): the majority of the campaigns cited by our interviewees are those related to narratives fostering polarization, questioning or rejecting of social values.
5. Economic impact (25%): One interviewee offers the perspective that certain corporations function as 'nation brands', and that the dissemination of discrediting campaigns can exert an influence on a nation´s economy, as well as its social cohesion. The other case mentioned is also related to the trade war experienced in the context of the distribution in the global market of the vaccines against the COVID-19.
6. Monetization (0%): This type of value vector associated with disinformation campaigns is not mentioned by any of the interviewees. Aguado and Gómez de Ágreda (2023) identify in their paper cases in which these campaigns have managed to produce direct revenue, generate social credit or increase demand for associative services.

As can be seen, the most concerning cases are those related to electoral interference processes. The most recent Annual National Security Report in Spain (Department of National Security, 2025) details how the Ministry of the Interior deployed a Coordination Network for Security in Electoral Processes during the 2023 voting rounds. This group, coordinated by the Department of National Security, focused on countering disinformation campaigns.

Furthermore, the Ministry of Foreign Affairs, European Union and Cooperation has also been involved in promoting positive information campaigns and the fight against disinformation through social media verification.

Notably, these efforts by state agencies, in which some of our interviewees are employed, have been focused on political influence. This may be why such cases come to mind when interviewees are asked about national security risks. Particularly if it is taken into account that the dissemination of information has historically been closely intertwined with political campaigns (Serrano-Puche *et al.*, 2018).

After inviting them to list cases in which disinformation campaigns have posed, or could potentially pose, a threat to national security, experts were asked whether they considered disinformation in Spain to be adequately addressed in relation to its potential impact. This notion of 'adequate consideration' was open-ended and closely related to the final block, in which experts were encouraged to propose actions, policies, or strategies to combat disinformation attacks.

Essentially, each respondent's vision of the problem and their own biases will determine the answer. The question has been added to the previous table to make it easier to understand. No differences are observed between academic and professional profiles. There are also no patterns between similar fields of work and study. However, some distinctions can still be observed in the emphases adopted by particular profiles. Professional profiles 1 and 2 recognize that, in Spain, disinformation is being considered in a way that is broadly appropriate to its potential impact, with professional profile 1 referring to the national cybersecurity strategy and warning that "the boundaries between protection and censorship are very blurred", and professional profile 2 similarly affirming that Spanish and EU responses became "appropriate for its potential impact" after the Catalan referendum. By contrast, professional profile 3 laments that "in Spain, we are a little behind the times", citing delayed EU recognition of electoral interference risks alongside inadequate journalistic and legislative re-

sponses, while professional profile 4 attributes this lag to Spanish society's "lack of awareness and critical consciousness", compounded by the deserved loss of trust in official sources. Among the academic profiles, academic profile 1 observes a disconnect between discursive emphasis—where "disinformation is central as if it were a major political concern"—and actual strategic action, both in government and companies, whereas academic profile 2 notes that, "although disinformation is not a new phenomenon", it now garners attention as a "national security issue". Academic profile 3 underscores democratic constraints, stressing that "it is very difficult to act with the tools that a democratic government has", where cyberspace protection is feasible but "you cannot censor" from other domains, and academic profile 4 concludes that "although certain initiatives have been taken, there is still much to be done", particularly "resolving the legal vacuum with AI".

3.3. "Disinformation wars": existence, scale, scope and damaging effects

Following the conceptualization of disinformation as a type of national security risk in block 2, an ad hoc term was introduced in the interview. The interviewees were asked to provide their understanding of the term 'disinformation wars', including the levels and scope of such activities, as well as relevant examples. The objective was to determine the experts' comprehension of the term, as they were unaware that it was a term invented for this study.

Notably, the interview was conducted following a discussion on national security risks. This factor seemingly influenced seven out of eight interviewees to accept the term, except for our academic expert on propaganda, who associates 'disinformation wars' with narratives in the context of war. This expert posits that propaganda has always been a pivotal strategy in war or conflict.

The remaining panel members, however, did adopt the term without hesitation, associating 'disinformation wars' with examples of propaganda on three occasions, issues related to social narrative or beliefs on three other instances, and finally, our defense and cyber defense professional profile with tactics or military movements in the cognitive and cyber domain.

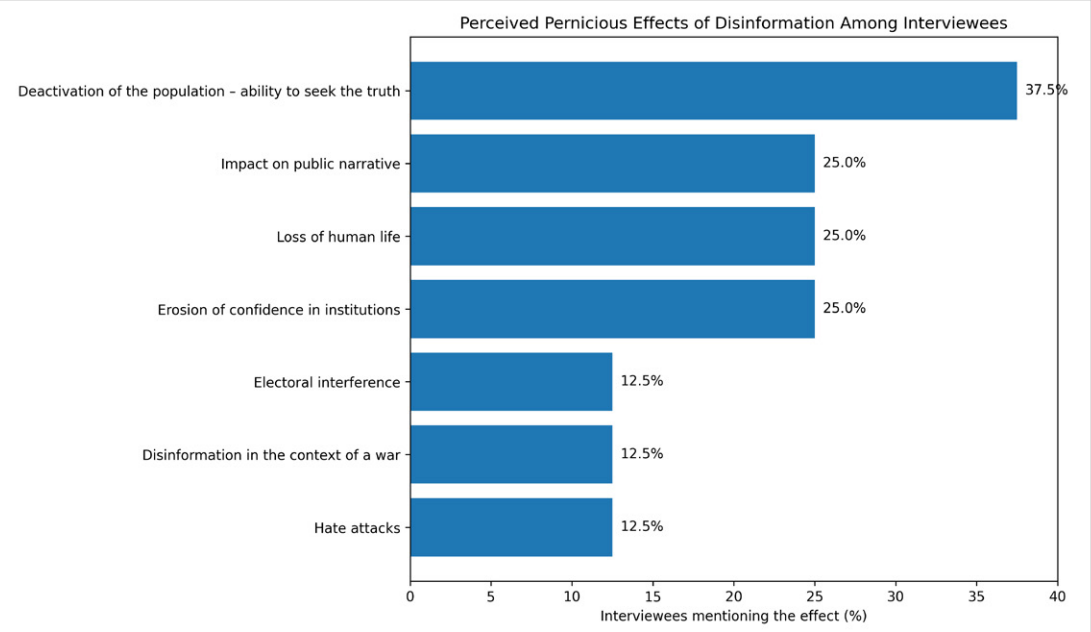
It is noteworthy that profiles such as the one who, in block one, showed reluctance to the link between disinformation and cybersecurity for fear that, by associating it with cybercrime, the escalation in the consideration of these phenomena would be greater, nevertheless buy the idea of 'disinformation wars' and provide use cases.

Initially, manifest thinking is reticent due to biases or sensitivities derived from the profession; however, as the interview progresses, implicit thinking becomes evident, relating cases to a higher measurement than 'crime ': 'war'.

For the second part of this block, experts were asked what they considered the most damaging effects of disinformation attacks. Contrary to initial expectations, the eight experts identified up to seven different types of risks, with little consensus among their responses.

The risks that were considered and identified as the most damaging of disinformation campaigns, together with the number of experts who indicated them, are as follows:

Figure 1. Perceived pernicious effects of disinformation among interviewees.



Source: Own formulation.

The variety of risks mentioned and the lack of consensus in choosing the most dangerous ones may demonstrate that the risks posed by disinformation campaigns to society are not well prioritized or that there is no consensus yet on this hierarchy. It should be noted that all the interviewees have either worked directly or indirectly with official documents related to disinformation campaigns over the last six

years, which rules out a gap in analytical skills on the part of the experts.

It is also important to highlight the relationship between the risks identified by our experts as the most pernicious and cybersecurity-related issues. In all these cases, vulnerabilities in digital ecosystems are exploited by malicious actors through various tactics and techniques (DISARM Foundation, 2024). The risks mentioned above, apart from the use of disinformation in the context of warfare, are the effects of such coordinated campaigns.

3.4. The role of artificial intelligence in disinformation campaigns

In the fourth segment of this study, the expert panel was consulted on the role of artificial intelligence in the nexus between cybersecurity and disinformation. In recent years, several authors have argued that the development of this tool has made it more necessary than ever to consider disinformation as a cyber threat (Kertysova, 2018; Khan, 2025; Mazurczyk *et al.*, 2024).

To this end, the interviewees were invited to consider this role as an amplifying effect of the phenomenon intimately associated with the cyber domain. The objective was to assess whether they spontaneously cited cases in which the link between disinformation and cybersecurity was more profound in type and proximity than they had indicated in the initial question.

The responses indicate a growing recognition among the participants of the nexus between disinformation and cybersecurity, a view that was not initially expressed to the same extent (Q1).

All interviewees emphasize the significance of artificial intelligence in the context of disinformation campaigns. Two of the professional profiles —one in defense and cyber defense and the other in OSINT and verification— highlight the detrimental implications of AI as a tool that amplifies disinformation and accelerates practices already in place, such as enhanced profiling for target identification, story generation, and automatic content dissemination through bots to achieve virality.

As the defense profile explained, AI enables "better profiling to identify and understand the targets of disinformation", while also making it possible to generate "narratives adapted to each of those profiles" and to automate dissemination "through bots to achieve virality"

On the other hand, the remaining interviewees balanced this by highlighting the potential benefits of AI as a countermeasure, emphasizing its capacity to detect and assess disinformation threats. As the national security profile put it, AI is "a tool for good and for bad in both cases", since in cybersecurity it helps "the bad guys create more complex attacks", but can also improve defensive response and enable advances in "message analysis" and sentiment analysis to counter disinformation.

3.5. Interdependencies between disinformation actors and cyberattack actors

In this block the interviewees are asked to consider how disinformation and cybersecurity might be related. The objective here was to explore the interviewees' awareness of these potential connections, demanding to explicit their views on the interrelationship between the actors involved, and inquiring whether improvements in one field might benefit the other.

Specifically, in question one, our interviewees were asked whether actors carrying out cyberattacks or cybercrime have any relationship with those developing disinformation campaigns and whether they were aware of such relationships, along with their reflections on the nature of these relationships and the contexts in which they occur. This information will help us to analyze any inconsistencies in discourse or gaps in analytical skills on the part of our interviewees.

Two of the eight interviewees identified a relationship between the actors who perpetrated cyberattacks and those who developed disinformation campaigns. They are professional profile 1 and professional profile 3.

The former defined the nature of the relationship between disinformation and cybersecurity as structural and its proximity as direct. This professional further elaborates that cybercriminal groups frequently assume a supportive role in the realm of disinformation, being hired by entities that seek to orchestrate such campaigns. Notably, these two actors are different subjects and the fundamental motivation behind this relationship is economic.

In defining the nature of the relationship between these actors, professional profile 3 characterizes it as circumstantial, with its duration being contingent upon the specific circumstances prevailing at a given moment. This is significant because, in response to a query regarding the identity of the actors involved, this profile indicates that they are frequently the same entities that utilize cyberattacks as instruments to expand the reach or impact of these disinformation campaigns, which, contradictorily involves a structural dimension.

The predominant consensus among five of the eight interviewees is that there is a relationship between actors who carry out cyberattacks and those who develop disinformation campaigns, although this is difficult to prove. Academic profile 1 notes that, in most cases, those who develop a disinformation campaign and those who carry out cybercrime attempt to keep their identity secret. In a similar line of argument, it is highlighted by professional profile 4 that the attributions made available to the public by the European Union are the only ones with which an informed assessment can be made. Furthermore, professional profile 2, who also draws attention to these attributions, points to instances of Russian units operating in conjunction with cyberattacks and disinformation campaigns.

Considering the response, professional profile 2 provides instances wherein the participants involved in both processes are not only related but the same. The presence of common actors across both processes, as highlighted by professional profile 3, introduces an inconsistency in the discourse, since their initial assessment characterized the cybersecurity-disinformation relationship as circumstantial and indirect.

Furthermore, when this interviewee indicated that the proximity between the two phenomena was indirect, the interviewee also pointed out that this relationship occurred through an intermediary factor,

never with a direct link. By contrast, the sharing of the same actors is a clear case of a direct link.

Academic profiles 2 and 4 also note that this relationship can occur depending on the case.

Finally, academic profile 3, who demonstrated a comprehensive understanding of the nexus between disinformation and cybersecurity, highlights the persistent decoupling between these two entities. This phenomenon arises due to corporate entities' strategic employment of cybercrime campaigns.

This perspective mirrors that of professional profile 1, which previously noted the existence of a contractual relationship between cybercriminal groups and those engaged in the development of disinformation campaigns. This can be interpreted as a deficiency in comprehending the inquiry, given that a contract is indeed a form of relationship.

Having established this, the analysis moves on to the second part of block 5, where respondents were asked whether improvements in cybersecurity could help in the fight against disinformation and whether improvements in the fight against disinformation could affect cybersecurity in any way.

In order to provide a comprehensive response to the question mentioned above, it is necessary to revisit the table showing the type of proximity that interviewees believe the cyber sphere has with the disinformation sphere. It has been established that proximity is direct when the characteristics of one sphere have an impact on the other, and indirect when this relationship does not exist, as there is no direct link between the two, only an intermediary factor that occasionally connects them.

It can be extrapolated logically from this that if an interviewee believes that the proximity between disinformation and cybersecurity is direct, it is reasonable to expect them to answer in a way that indicates a positive effect on both spheres if one improves, and vice versa. The responses of the panel of experts have been considered in turn and point by point:

Table 4. Perceptions of the disinformation-cybersecurity relationship among expert profiles.

Profile	Perceived relationship disinformation-cybersecurity	Cybersecurity improvements help fight disinformation?	Anti-disinformation efforts improve cybersecurity?	Notes / remarks
Professional profile 1	Direct	Yes	No	Technical / defense bias
Professional profile 2	Indirect	Unclear / reluctant	Yes	Communication / OSINT bias
Professional profile 3	Direct	Yes	Yes	Sees mutual reinforcement
Professional profile 4	Indirect	No	No	Considers both fields separate
Academic profile 1	Direct	Yes	Yes	Mutual, consistent view
Academic profile 2	Indirect	Yes	Yes (with uncertainty)	Reluctant; legal concerns
Academic profile 3	Direct	Yes	No	Technical focus; undervalues social side
Academic profile 4	Direct	Yes	Yes	Mutual reinforcement via protection & education

Source: Own formulation.

Note: N = 8. This table compares the initially stated perception of the disinformation-cybersecurity relationship with respondents' views on whether improvements in one field may benefit the other. The labels in the "Notes / remarks" column are analytical groupings assigned by the researchers on the basis of the interview material; they do not represent participants' self-descriptions.

Beyond the descriptive distribution shown in Table 4, the interviews reveal two opposite patterns of field-specific bias. The patterns summarized in Table 4 do not reflect participants' self-perceptions, but analytical regularities identified by the researchers when comparing the initial characterization of the link with subsequent answers on possible mutual reinforcement between both fields. On the one hand, technically oriented experts in defense and cybersecurity (professional profile 1 and academic profile 3) conceive the relationship between disinformation and cybersecurity as direct, but essentially one-way: improvements in cybersecurity are seen as a key tool against disinformation, whereas advances in the fight against disinformation are perceived as having no meaningful impact on cybersecurity. This asymmetry suggests a partial undervaluation of social and communicative capacities in addressing the problem.

On the other hand, experts with a communication and OSINT background (notably professional profile 2) tend to invert this asymmetry. While defining the relationship as indirect and expressing reluctance to focus on cybersecurity, they clearly state that improvements in the fight against disinformation do strengthen cybersecurity, for instance by protecting citizens from scams and data theft. As this interviewee puts it, "a cyberattack always implies a cybercrime, and this is, from my point of view, a much more serious level on the scale of problems," which helps explain their hesitation to grant cybersecurity a central role in disinformation-related debates.

A third group of respondents (professional profile 3 and Academic Profiles 1 and 4) consistently endorse a mutually reinforcing relationship: they argue that strengthening cybersecurity protects the infrastructures through which disinformation circulates, while improving citizens' resilience and media literacy against disinformation can also mitigate cyber threats. Conversely, professional profile 4 and academic profile 2 remain more skeptical, describing the link as indirect or even stating that "they are completely separate phenomena". In the case of the legal expert (academic profile 2), this reluctance is explicitly connected to concerns that a tight coupling between disinformation and cybersecurity could legitimize regulatory tools that might unduly restrict freedom of expression.

3.6. Potential solutions

The final block is also aligned with the concluding question. In this section, the experts were invited to identify the actions, policies, or strategies they consider necessary to combat disinformation. A comprehensive understanding of the focal points of each profile when discussing mitigation is instrumental in evaluating the extent of their comprehension of the phenomenon and the analytical perspective they adopt.

The responses, organized according to the profiles, are presented below:

Table 5. Mitigation strategies against disinformation proposed by expert profiles.

Profile	Main mitigation strategies against disinformation	Key themes
Professional profile 1	Promote a societal attitude shift towards proactive personal security and autonomy.	Individual responsibility, behavioral change, personal security culture.
Professional profile 2	Advance cybersecurity and defense; provide education and training for civil servants; implement a multifaceted strategy across different domains.	Cybersecurity measures, public-sector training, multidimensional approach.
Professional profile 3	Promote critical thinking in schools; support a free and robust press; regulate social media platforms to monitor, tag and remove fake news; foster international cross-border cooperation.	Education, media freedom, platform regulation, international cooperation.
Professional profile 4	Launch awareness-raising and sensitization initiatives; foster public trust in institutions; promote critical thinking, especially among minors...	Awareness, institutional trust, critical thinking (youth focus).
Academic profile 1	Empower citizens to understand digital environments through education; secure political party agreements and public commitments; maintain institutional pressure on tech and social media platforms to enhance transparency.	Digital literacy, political/institutional commitments, platform transparency.
Academic profile 2	Prioritize identifying and deactivating bots and analogous entities; notes strong limits of legal recourse when the source is human.	Technical detection (bots), legal constraints, enforcement limits.
Academic profile 3	Integrate cybersecurity components from early education through university; establish retraining programs for adults.	Lifelong education, cybersecurity in curricula, adult retraining.
Academic profile 4	Adopt a holistic approach combining education, transparency, regulation of online platforms, promotion of diverse media and professionals, research, and accountability.	Holistic strategy, regulation, media pluralism, research, accountability.

Source: Own formulation.

Beyond the individual profiles, two cross-cutting patterns emerge from the proposed mitigation strategies. First, even the experts who are initially most reluctant to acknowledge a strong link between disinformation and cybersecurity (Professional Profile 2 and Academic Profile 2) end up assigning a central role to cybersecurity in their proposed responses. Both advocate technical measures such as improving cyber defense capabilities, training civil servants, and identifying or deactivating bots and analogous entities. This shift suggests that, once the interview progresses and the connections between disinformation and cyber threats are made explicit, cybersecurity is spontaneously reframed by these experts as an indispensable mitigation tool, despite their earlier reservations grounded in concerns about freedom of expression and the perceived hierarchy of problems.

Second, education appears as a recurrent axis across most interviews, often framed in terms of digital literacy, critical thinking, awareness-raising and lifelong training. This prominence reflects a clear preference for detection (and education) centered approaches focused on the content and consequences of disinformation. However, such a perspective tends to leave in the background other crucial dimensions of the phenomenon, particularly the role of actors who pursue disinformation campaigns for political, strategic or economic purposes

(Aguado & Gómez de Ágreda, 2023). In this sense, the emphasis on education, while necessary, risks underestimating the structural drivers and strategic intent that sustain contemporary disinformation ecosystems.

4. Conclusions and next steps

This work examines the link between disinformation and cybersecurity from the perspective of experts who work in at least one of these two domains and are, in all cases, directly involved with disinformation.

The interviews reveal a clear discrepancy in how experts from communication and law, on the one hand, and those from security and cybersecurity, on the other, understand the nature and proximity of the relationship between disinformation and cybersecurity. Beyond this initial divergence, it is striking how consensus gradually builds as the interview progresses and participants are confronted with less explicit connections between both fields (e.g. national security implications, interrelations between actors). Despite some participants' initial rejection of a strong link, as the conversation moves into this more complex territory and interviewees are guided through concrete examples, these connections begin to surface and certain discursive inconsistencies emerge.

A critical reading of the responses allows us to identify a set of factors that reveal the gap between manifest and latent thinking. Epistemic biases between fields —that is, cognitive deviations affecting our ability to acquire and process knowledge objectively (Bueter, 2022)— are clearly present. Such biases are frequently observed across domains of knowledge, and our material offers several illustrative cases.

Experts in communication and law appear particularly sensitive to freedom of expression and access to information, repeatedly expressing concern that excessive reliance on technological tools or restrictive policies may infringe these rights. Those whose work is not directly related to cybersecurity tend to equate cybersecurity almost exclusively with cybercrime, which contributes both to an exaggerated perception of the 'severity' threshold needed to take disinformation seriously, and to a narrow, crime-centered understanding of the cyber domain. Their responses also reveal a stereotyped image of cybersecurity actors —often reduced to the figure of an isolated individual with a hood and an Anonymous mask— and, more broadly, a conception of cybersecurity as a highly specialized and isolated sector with little or nothing to do with disinformation.

By contrast, our two experts from the security and cybersecurity field, who also work directly on disinformation, show that a more detailed and comprehensive understanding of cybersecurity makes it easier to perceive and articulate relationships between the two phenomena. This suggests that awareness of the link between disinformation and cybersecurity depends to a significant extent on the level and breadth of prior knowledge.

However, stereotyping operates in both directions. In the section where cybersecurity profiles are asked about the interrelation between actors and potential mutual support between both fields, they express reluctance to accept that improvements in the fight against disinformation can benefit cybersecurity, thereby undervaluing a field in which communication experts, by contrast, offer clear and concrete proposals for how such support could be realized.

On the other hand, all eight interviewees strongly emphasize detection and education throughout their interviews, which reflects a view of disinformation centered on messages and their effects. Numerous academic works note that this has so far been the dominant perspective (Arsenault, 2020; Bechmann, 2020; Kapantai *et al.*, 2021). However, this is a limited approach that implicitly downplays the role of the actors involved and their political, strategic and economic motivations (Aguado & Gómez de Ágreda, 2023), especially in electoral contexts where disinformation campaigns have been extensively documented (Sánchez del Vas et al., 2025).

In conclusion, the reported absence of a connection between disinformation and cybersecurity can be understood as the result of disciplinary biases that constrain the understanding of a complex phenomenon. These differences between experts from distinct fields of knowledge within the same broader area are linked to the lack of consolidation and cohesion of concepts in an emerging field (Kapantai *et al.*, 2021), that is, to the absence of a 'common language'.

This study not only identifies several avenues for future research, but also shows that the interview dynamic itself encouraged experts to move beyond their disciplinary comfort zones. As participants were progressively exposed to perspectives and connections beyond their home field, their positions converged and they began to recognize the added value of other disciplinary approaches. This points directly to the need to construct the kind of interdisciplinarity required to address a complex phenomenon such as disinformation. In this sense, further work on consolidating shared concepts and definitions is essential, both as a precondition and as a result of this interdisciplinary dialogue, in order to facilitate more systematic collaboration in the fight against disinformation campaigns.

As Caramancion (2020) argues, it is crucial that disinformation be formally recognized and categorized as a cybersecurity threat. This would enable a more precise analysis of its nature and the development of appropriate mitigation strategies.

Finally, to address the challenge of disinformation effectively, it is necessary to adopt a comprehensive approach that considers not only technical and content-related aspects, but also the broader social, political and technological context in which the phenomenon unfolds. Only under these conditions can effective strategies be developed to mitigate its impact and strengthen societies' resilience against this multifaceted threat.

4.1. Limitations and future directions

Future work may benefit from larger, more structured samples to enable comparative analyses across countries. Combining qualitative approaches with quantitative surveys or experimental designs would further strengthen generalizability.

The diversity of profiles and the evolving nature of disinformation and cybersecurity —particularly with

the rapid integration of AI tools— also present ongoing challenges warranting continued investigation. Despite these considerations, the findings offer significant interdisciplinary insights that enrich both disinformation studies and cyber threat analysis.

5. Funding and Support

This work was funded by the Spanish Research Agency (AEI), Ministry of Science and Innovation (MCIN) (MCIN/AEI/10.13039/501100011033), under project PID2024-156890OP-I00 and predoctoral grant PRE2024-003406.

6. Authors' contribution

Conceptualization	Ideas; formulation or evolution of overarching research goals and aims.	Authors 1, 2, 3
Data curation	Management activities to annotate (produce metadata), scrub data and maintain research data (including software code, where it is necessary for interpreting the data itself) for initial use and later re-use.	Authors 1, 2
Formal analysis	Application of statistical, mathematical, computational, or other formal techniques to analyse or synthesize study data.	Authors 1, 2, 3
Funding acquisition	Acquisition of the financial support for the project leading to this publication.	Author 2
Investigation	Conducting a research and investigation process, specifically performing the experiments, or data/evidence collection.	Author 1
Methodology	Development or design of methodology; creation of models.	Authors 1, 2
Project administration	Management and coordination responsibility for the research activity planning and execution.	Author 1
Resources	Provision of study materials, reagents, materials, patients, laboratory samples, animals, instrumentation, computing resources, or other analysis tools.	Authors 1, 2, 3
Software	Programming, software development; designing computer programs; implementation of the computer code and supporting algorithms; testing of existing code components.	Author 3
Supervision	Oversight and leadership responsibility for the research activity planning and execution, including mentorship external to the core team.	Author 2
Validation	Verification, whether as a part of the activity or separate, of the overall replication/reproducibility of results/experiments and other research outputs.	Authors 2, 3
Visualization	Preparation, creation and/or presentation of the published work, specifically visualization/data presentation.	Author 1
Writing / original draft	Preparation, creation and/or presentation of the published work, specifically writing the initial draft (including substantive translation).	Author 1
Writing / review & editing	Preparation, creation and/or presentation of the published work by those from the original research group, specifically critical review, commentary or revision —including pre— or post-publication stages.	Authors 2, 3

7. Statement on the use of artificial intelligence

Artificial intelligence has been used in this article exclusively for grammar and English expression correction. The tool employed was ChatGPT (OpenAI), which was used solely for English language revision of text already drafted by the authors. It was not involved in data analysis, interpretation of findings, or the formulation of the study's conclusions.

8. References

Aguado, J. M., & Gómez de Ágreda, A. (2023). Disruptive conflict-based innovation and perverse economic logics: the case of the disinformation ecosystem. *Communication at 2023 conference of the International Association for Media and Communication Research*, IAMCR 2023, Lyon, Francia.

Arsenault, A. (2020). *Microtargeting, automation, and forgery: Disinformation in the age of artificial intelligence* [Major research paper, University of Ottawa]. uO Research. https://ruor.uottawa.ca/server/api/core/bitstreams/11d2b66c-cdab-45bc-b150-4fa82973e322/content

Bechmann, A. (2020). Tackling disinformation and infodemics demands media policy changes. *Digital journalism*, 8(6), 855-863. https://doi.org/10.1080/21670811.2020.1773887

Ben Aharon, E. (2023). Methodological and epistemological reflections on elite interviews and the study of Israel's intelligence history: Interview with Efraim Halevy. *Intelligence and National Se-*

curity, 38(1), 111-127. https://doi.org/10.1080/02684527.2022.2095600

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

Broda, E., & Strömbäck, J. (2024). Misinformation, disinformation, and fake news: Lessons from an interdisciplinary, systematic literature review. *Annals of the International Communication Association*, 48(2), 139-166. https://doi.org/10.1080/23808985.2024.2323736

Bueter, A. (2022). Bias as an epistemic notion. *Studies in History and Philosophy of Science*, 91, 307-315. https://doi.org/10.1016/j.shpsa.2021.12.002

Caramancion, K. M. (2020). An exploration of disinformation as a cybersecurity threat. *In 2020 3rd International Conference on Information and Computer Technologies (ICICT)* (pp. 440-444). IEEE. https://doi.org/10.1109/ICICT50521.2020.00076

Cea, N., Fernández Torres, M. J., & Teruel Rodríguez, L. (2023). Tratamiento del fenómeno de la desinformación en la prensa española: Un análisis de su evolución. *Estudios sobre el Mensaje Periodístico*, 29(4), 881-891. https://doi.org/10.5209/esmp.88087

De Miguel Pascual, R. (2005). La entrevista en profundidad a los emisores y los receptores de los medios. En M. R. Berganza Conde & J. A. Ruiz San Román (Coords.), *Investigar en comunicación: Guía práctica de métodos y técnicas de investigación social en comunicación* (pp. 251-264). McGraw-Hill/Interamericana de España.

DISARM Foundation. (2025). *DISARM Red Framework*. Retrieved February 6, 2025, from https://www.disarm.foundation/framework

Department of National Security. (2020). *Informe anual de Seguridad Nacional 2019* [2019 National Security Annual Report]. Presidency of the Government of Spain. https://www.dsn.gob.es/es/publicaciones/informes-anuales/IASN2020

Department of National Security. (2025). *Informe anual de Seguridad Nacional 2024* [2024 National Security Annual Report]. Presidency of the Government of Spain. https://www.dsn.gob.es/es/publicaciones/informes-anuales-IASN2024

Kapantai, E., Christopoulou, A., Berberidis, C., & Peristeras, V. (2021). A systematic literature review on disinformation: Toward a unified taxonomical framework. *New media & society*, 23(5), 1301-1326.

Kertysova, K. (2018). Artificial intelligence and disinformation: How AI changes the way disinformation is produced, disseminated, and can be countered. *Security and Human Rights*, 29(1-4), 55-81.

Khan, U. K. A. B. G. (2025). Disinformation security at the nexus of cybersecurity and AI: Defending digital ecosystems against automated deception. World Journal of Advanced Engineering Technology and Sciences, 15(2), 2618-2625. https://doi.org/10.30574/wjaets.2025.15.2.0813

López, A. B., García-Alcaraz, T. G., Tárraga, M. F., Tudela, A. D. C., González, F. S., Galindo, J. P., Ruipérez-Valiente, J. A., & Martínez Pérez, G (2025). EUCINF: EUropean Cyber and INFormation warfare toolbox. Actas de las X Jornadas Nacionales de Investigación en Ciberseguridad (pp. 130-133). Universidad de Zaragoza.

Mazurczyk, W., Lee, D., & Vlachos, A. (2024). Disinformation 2.0 in the age of AI: A cybersecurity perspective. *Communications of the ACM*, 67(3), 36-39. DOI: 10.1145/3624721

Mirza, M. S., Begum, L., Niu, L., Pardo, S., Abouzied, A., Papotti, P., & Pöpper, C. (2023). Tactics, threats & targets: Modeling disinformation and its mitigation. In *Proceedings of the 2023 Network and Distributed System Security Symposium (NDSS)*. Internet Society. https://doi.org/10.14722/ndss.2023.23657

MITRE. (2025). MITRE ATT&CK® version 18.1 [Knowledge base of adversary tactics and techniques]. The MITRE Corporation. https://attack.mitre.org/

NATO Strategic Communications Centre of Excellence. (2025). Virtual Manipulation Brief 2025 (VMB 2025). https://www.stratcomcoe.org/

Palacios, S. P. I., & Rubio, K. L. A. (2003). *La entrevista en profundidad: teoría y práctica*. Universidad Autónoma de Tamaulipas.

Rodríguez-Fernández, L., & Establés, M. J. (2023). Impacto de la desinformación en las relaciones públicas: Aproximación a la percepción de los profesionales. *Estudios sobre el Mensaje Periodístico*, 29(4), 843-853. https://doi.org/10.5209/esmp.88661

Sánchez del Vas, R., Ruiz Incertis, R., García Acosta, D., & Magallón Rosa, R. (2025). *Análisis de la campaña de desinformación en las elecciones brasileñas de 2022*. Doxa Comunicación. Revista Interdisciplinar de Estudios de Comunicación y Ciencias Sociales, 41, 231-255. https://doi.org/10.31921/doxacom.n41a2320

Serrano-Puche, J., Fernández, C. B., & Rodríguez-Virgili, J. (2018). Political information and incidental exposure in social media: The cases of Argentina, Chile, Spain, and Mexico. *Doxa Comunicación*, 27, 19-42. https://doi.org/10.31921/doxacom.n27a1

Vasu, N., Ang, B., Teo, T.-A., Jayakumar, S., Faizal, M., & Ahuja, J. (2018, January*). Fake news: National security in the post-truth era [Policy report]*. S. Rajaratnam School of International Studies. https://www.rsis.edu.sg/wp-content/uploads/2018/01/PR180313_Fake-News_WEB.pdf

Von Soest, C. (2023). Why do we speak to experts? Reviving the strength of the expert interview method. *Perspectives on Politics*, 21(1), 277-287. https://doi.org/10.1017/S1537592722001116

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making* [Report]. Council of Europe. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

World Economic Forum. (2024). The global risks report 2024: 19th edition. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Teresa García de Alcaraz Ruiz. Teresa García de Alcaraz Ruiz is a predoctoral researcher at the University of Murcia, where she is developing her doctoral thesis on disinformation, cybersecurity, and the analysis of related ecosystems. She is affiliated with the Cybersecurity and Data Science Lab and participates in national and European research projects related to cybersecurity and generative artificial intelligence. Her academic background includes degrees in Journalism and in Documentation and Information, as well as a master's degree in Digital Content. ORCID: https://orcid.org/0009-0009-0586-5664

Juan Miguel Aguado Terrón. Juan Miguel Aguado is a Full Professor of Journalism at the University of Murcia and holds a PhD in Information Sciences from the Complutense University of Madrid. He has taught at universities in Poland, the United Kingdom, and Spain, and has an extensive research career in communication, technology, and digital culture. He is the author of several monographs and more than forty articles in international scientific journals. Founder of the Mobile Media Research Lab, he has led numerous research projects on mobile communication and digital transformation, and currently leads the project "CreAItive MEDIA: Artificial Creativity in Media Ecosystems," funded by the Spanish Research Agency (PID2024-156890OB-I00, 2025-2027). Between 2016 and 2019, he served as Director General of Radio Televisión de la Región de Murcia and has held prominent positions in national and international organizations in the audiovisual sector. ORCID: https://orcid.org/0000-0002-8922-3299

José Antonio Ruiperez Valiente. José Antonio Ruipérez Valiente is an Associate Professor in the Department of Information and Communications Engineering at the University of Murcia. He has taught at the Complutense University of Madrid, where he also held a Juan de la Cierva research fellowship, and was a postdoctoral researcher at MIT. His work covers the study of digital technologies applied to learning, human-computer interaction, and, more recently, research on disinformation and cybersecurity. ORCID: https://orcid.org/0000-0002-2304-6365