Revista científica editada por la Facultad de Información y Medios Audiovisuales de la Universidad de Barcelona
ISSN 1575-5886

BiD 55 (diciembre 2025)
DOI: 10.1344/bid2025.55.07

ORIGINAL ARTICLE

Major Academic Publishers on Telegram Channels: An Approach to Fake Channel Detection Using ChatGPT and DeepSeek

Principales editores científicos en los canales de Telegram: una aproximación a la detección de *fake channels* con ChatGPT y DeepSeek

Principals editors científics als canals de Telegram: una aproximació a la detecció de canals falsos amb ChatGPT i DeepSeek

Víctor Herrero-Solana
Universidad de Granada
victorhs@ugr.es

Carlos Castro-Castro
Universidad de Granada
ccastro@ugr.es ✉

Received: 10-09-2025
Accepted: 07-11-2025

Recommended citation

Herrero-Solana, Víctor, & Carlos Castro-Castro (2025). Principales editores científicos en los canales de Telegram: una aproximación a la detección de *fake channels* con ChatGPT y DeepSeek. BiD, 55. https://doi.org/10.1344/BID2025.55.07

Abstract

Objectives: To identify the existence of fake channels on Telegram that impersonate major academic publishers, evaluate the effectiveness of Large Language Models (LLMs), specifically ChatGPT and DeepSeek, for their detection, analyze the web sources used by these models, and determine the potential existence of geographical biases in these sources.

Methodology: Selection of 13 major academic publishers from the SCImago portal: Elsevier, Springer, Wiley-Blackwell, Routledge, OUP, de Gruyter, Brill, CUP, IEEE, Hindawi, World Scientific, Nature, and Thieme. Identification of 37 associated Telegram channels, and application of a standardized prompt to ChatGPT and DeepSeek to evaluate the authenticity of each channel, with the web search function enabled. Comparative analysis of the models' responses and verification through manual classification.

Results: It was identified that 78.38% of the analyzed channels were fraudulent. Both models showed high effectiveness in detecting fake channels but significant limitations in validating legitimate channels. Methodological differences were observed: DeepSeek adopted a contextual approach, while ChatGPT required explicit verification. The analysis of web sources revealed that DeepSeek prioritized cybersecurity content, whereas ChatGPT predominantly used institutional sources and social media, with a clear predominance of Western sources in both cases.

Keywords

Telegram; fake channels; academic publishers, LLM, ChatGPT;, DeepSeek; misinformation detection; source verification.

Resumen

Objetivos: Identificar la existencia de canales falsos en Telegram que suplantan a grandes editoriales académicas, evaluar la efectividad de los Modelos de Lenguaje a Gran Escala (LLMs), específicamente ChatGPT y DeepSeek, para su detección, analizar las fuentes web utilizadas por estos modelos y determinar la posible existencia de sesgos geográficos en dichas fuentes.

Metodología: Selección de 13 grandes editoriales académicas del portal SCImago: Elsevier, Springer, Wiley-Blackwell, Routledge, OUP, de Gruyter, Brill, CUP, IEEE, Hindawi, World Scientific, Nature y Thieme. Identificación de 37 canales de Telegram asociados y aplicación de un prompt estandarizado a ChatGPT y DeepSeek para evaluar la autenticidad de cada canal, con la función de búsqueda web activada. Análisis comparativo de las respuestas de los modelos y verificación mediante clasificación manual.

Resultados: Se identificó que el 78,38% de los canales analizados eran fraudulentos. Ambos modelos mostraron una alta efectividad en la detección de canales falsos, pero limitaciones significativas para validar canales legítimos. Se observaron diferencias metodológicas: DeepSeek adoptó un enfoque contextual, mientras que ChatGPT requirió una verificación explícita. El análisis de las fuentes web reveló que DeepSeek priorizó contenido de ciberseguridad, mientras que ChatGPT utilizó predominantemente fuentes institucionales y redes sociales, con un claro predominio de fuentes occidentales en ambos casos.

Palabras clave

Telegram; canales falsos; editores académicos; LLM; ChatGPT; DeepSeek, detección de desinformación; verificación de fuentes.

Resum

Objectius: Identificar l'existència de canals falsos a Telegram que suplanten les principals editorials acadèmiques, avaluar l'eficàcia dels models grans del llenguatge (LLM), ChatGPT i DeepSeek, per a la seva detecció, analitzar les fonts web utilitzades per aquests models i determinar la possible existència de biaixos geogràfics en aquestes fonts.

Metodologia: Selecció de 13 grans editorials acadèmiques a partir del portal SCImago: Elsevier, Springer, Wiley-Blackwell, Routledge, OUP, de Gruyter, Brill, CUP, IEEE, Hindawi, World Scientific, Nature i Thieme. Identificació de 37 canals de Telegram associables i aplicació d'un prompt estandarditzat a ChatGPT i DeepSeek per avaluar l'autenticitat de cada canal, activant la funció de cerca web. Anàlisi comparativa de les respostes dels models i verificació mitjançant classificació manual.

Resultats: Es va identificar que el 78,38% dels canals analitzats eren fraudulents. Ambdós models van mostrar alta efectivitat en la detecció de canals falsos, però limitacions significatives en la validació de canals reals. Es van observar diferències metodològiques: DeepSeek va adoptar un criteri contextual, mentre que ChatGPT va requerir verificació explícita. L'anàlisi de fonts web va revelar que DeepSeek va prioritzar continguts de ciberseguretat, mentre que ChatGPT va utilitzar predominantment fonts institucionals i xarxes socials, amb clar predomini de fonts occidentals en ambdós casos.

Paraules clau

Telegram, canals falsos, editors acadèmics, LLM, ChatGPT, DeepSeek, detecció de desinformació; verificació de fonts.

1. Introduction

The instant messaging application Telegram has long since transcended its initial function as a person-to-person messaging service, becoming a robust technology for global information exchange. Unlike traditional social networks, users typically associate it with intimate communication (Dargahi et al., 2017), overlooking the fact that channels on this service can constitute a substantial source of information. The lack of centralized control over channel publication makes it easy for users to be confused about the origin and responsibility of these channels, as has already been demonstrated for the case of the Spanish press (Herrero and Castro, 2022).

The proliferation of fake news and misinformation has become a significant concern in the digital era. With the rise of social media platforms and the increasing ease of information dissemination, the spread of misleading content poses serious threats to public opinion, democratic processes, and social harmony (Shu et al., 2017). In this context, Large Language Models (LLMs) have emerged as promising tools for combating misinformation, thanks to their deep world knowledge and powerful reasoning capabilities. Recent research has demonstrated that fine-tuned pre-trained models, both older models such as BERT and RoBERTa and more advanced LLMs, can achieve remarkable results in fake news detection without requiring extensive auxiliary data (Flores-Vivar and García-Peñalvo, 2023). These models have shown particular efficacy through prompting strategies, especially chain-of-thought reasoning, which significantly improves performance in fact-verification tasks (Chen and Shu, 2024).

For the present study, two LLMs representative of the current landscape were selected: ChatGPT and DeepSeek. The selection of ChatGPT is due to its being the first to make a significant impact (and attract considerable attention) at the end of 2022 (Thorp, 2023) and its current dominant position in the language model market. According to various market analyses, ChatGPT maintains a share exceeding 80% among generative AI chatbots, consolidating itself as the most widely used LLM by both individual users and enterprises (StatCounter 2025). Its widespread adoption and recognition make it the natural reference point for evaluating fraudulent content detection capabilities.

The inclusion of DeepSeek, in turn, responds to its singular relevance at the time of designing this experiment. In January 2025, this Chinese startup burst onto the international media scene by presenting its R1 model, which demonstrated capabilities comparable to those of its Western competitors, but developed under significant restrictions on access to advanced hardware. U.S. export control policies, implemented since October 2022, severely restricted manufacturers such as Nvidia from selling their most powerful chips (H100 and A100) to Chinese companies. DeepSeek managed to train its models using H800 chips, a version with limited performance designed specifically for the Chinese market. Rather than limiting themselves to standard use of Nvidia's framework (CUDA), its engineers resorted to very low-level programming in PTX—the assembly-like language underlying CUDA—to maximize the potential of these chips (Chen, 2025). The impact of its emergence even generated a sharp stock market decline for Nvidia itself: nearly $600 billion in a single day (Carew et al., 2025). This case represents an interesting methodological counterpoint to ChatGPT, being a model developed under technological restrictions that nevertheless achieves competitive performance levels.

2. Theoretical Framework

2.1. Telegram Channels

The success of WhatsApp as an alternative to SMS when the use of Internet-connected touchscreen mobile phones began to become widespread marked the beginning of the growth of instant messaging applications. The emergence of WeChat in China and applications such as Telegram and Signal, presented as more transparent and secure tools, gave rise to a new communicative environment. The various advances of different applications have mutually enriched each other's capabilities, contributing to a constant increase in users (Gregorio et al., 2017).

The introduction of channels on Telegram in 2015 marked the emergence of a new form of unidirectional communication that enables the dissemination of news, entertainment content, official communications, etc., to unlimited global audiences (Kitsa 2023). The incorporation of new features since then has been constant, including message editing (which allows for error correction or information updates after publication), basic analytics tools for tracking message performance, improved management capabilities, and diversified formats and tools. Telegram has not been a standard application, as some of its decisions regarding cryptography and security are singular (Jakobsen, 2015). Its security architecture is presented as a paramount value for the robustness of the tool itself (Wardle and Derakhshan, 2017).

Telegram has been incorporated into media information activities (Sánchez and Martos, 2020), and the robustness of channels for information dissemination has been verified (Sedano and Palomo, 2018). Telegram has carved out a niche in the current media landscape by establishing itself as an alternative channel for news consumption. It has been demonstrated that trust in journalistic brands plays a crucial role in the selection of information sources on this platform (Martos and Sánchez, 2024). Its flexibility has enabled the development of informational and communicative solutions in such extraordinary situations as the Ukraine war, where new communicative formats have been created (Steblyna, 2024). It has also been used by university institutions in Spain and Latin America for disseminating their information (Cisternas et al., 2022). This has not occurred to the same extent in purely commercial environments. Telegram has proven robust for supporting documentary information systems and, at the same time, generating communicative environments at different levels. These capabilities have been verified in various formats (Mohammed et al., 2024). The variety of these formats, the robustness of its storage system, and its content dissemination capacity have been successfully used in language learning experiences and linguistic skill reinforcement (Abu-Ayfah, 2020).

Telegram provides a structured model for use in social interaction and expert moderation (Ghaffari et al., 2017). These strengths have not yielded the desired results in fields such as healthcare. In 2020, during the pandemic, Telegram made an offer for health authorities worldwide to verify their official channels. Surprisingly, the initiative was followed by only about twenty countries and did not have significant traction. Paradoxically, under those circumstances, it was the tool chosen by many organizations to disseminate their information during this crisis (López, 2020). During that same period, faced with the demand for remote work, Telegram notably improved its video communication tools, both in chats and in groups and channels, achieving capabilities even greater than some of the most popular streaming platforms, developing as a hybrid system that has notably expanded communicative capabilities (Dargahi et al., 2021).

Telegram channels have progressively become true dissemination platforms (Willaert, 2023). The refinement of advanced permissions for administrators equips them with capabilities to assign roles and manage in a granular manner who can publish, edit, pin, or delete messages, functionally converting them into editors (Gregorio, 2020). The added possibility of associating discussion groups with channels, combined with improved analytical and statistical tools, has also allowed for instruments to evaluate the reach and interaction of publications (La Morgia et al., 2023).

Telegram's search system mixes the location of channels by words contained in their title with the location of words in the content of all subscribed channels. This proves very fast and effective for locating content in subscribed channels but very confusing and unreliable for precise channel location (Jalilvand and Neshati, 2020).

In Telegram's 2024 updates, everything related to mini apps on its bot platform was notably strengthened, with growing activity around rewards and monetization of commercial services and activities. The success of these new activity areas has opened a line of action that, in the first updates of 2025, is being projected onto channels. The launch of the third-party verification system presented by Telegram in the year's first update is good proof of this. This new system for combating scams and misinformation adds to the traditional checkmark the possibility for official services external to Telegram to verify accounts and chats. Channels or accounts verified through this method will be able to display a unique icon next to their name, and by clicking on it, users can see which service performs the certification and the reason. In the March 2025 update, utilities for inbox control were added. These allow setting a fee for incoming messages from users who are not among the contacts, facilitating total control over the inbox. Users will be able to earn stars (the payment system used in mini apps), filter unwanted messages, and avoid inbox overload. This configuration can also be applied to group chats and channel conversations to keep interactions focused and spam-free, which helps their owners monetize their community and earn stars from meaningful conversations (Telegram, 2025). All these measures enable increasing transparency and trust in published content, but they will only bear fruit if the media, institutions, and scientific community make use of them.

It is undeniable that these utilities have opened opportunities and new vulnerabilities, posing challenges that need to be addressed (Sušánka and Kokeš, 2017). The fact that anyone can create a public Telegram channel, imitate the image of an original, name it, and even feed it with messages from any source means the system has not shown robustness, since channel verification has not become widespread. Although numerous 'theoretically official' channels exist, even linked from their websites, many appear on Telegram without the official verification checkmark (Herrero and Castro, 2022). Sometimes, channels with identical names appear, making it difficult to verify their official nature, as they even reproduce content from the RSS feeds of the media and organizations themselves (La Morgia et al., 2023). There is evidence that the capabilities described allow for easy dissemination of misinformation due to privacy and anonymity preservation. This has resulted in the proliferation of fake channels, as was notably evidenced after the pandemic (Díez et al., 2021).

In recent years, following several episodes of media resonance, it appears that relations with government bodies in different countries are becoming more fluid and more agreements are being reached with regulators. Good proof of this is the removal of millions of harmful publications and channels every day, the publication of daily transparency reports, and direct lines with NGOs to process moderation requests more quickly (Durov, 2024).

The very nature of channels, their ease of creation, and the nonexistent moderation (except for verification or removal in response to a complaint) make the dissemination of misinformation an inevitable fact (Herasimenka et al., 2023). Its impact is especially concerning in the scientific domain due to identity impersonation problems through the misuse of publisher names and official logos to gain instant credibility (Wardle and

Derakhshan, 2017). Informational manipulation through the dissemination of false, manipulated, or incomplete studies can negatively influence academic debates and political decisions (Cho et al., 2019). The inevitable erosion of trust, by confusing users, can damage the credibility of science and academic institutions (Allcott and Gentzkow, 2017).

The nature of Telegram channels allows for generating information databases to analyze them and obtain reliable results that can be evaluated. However, the task of evaluating the results of quantitative analyses has until now required the participation of human analysts (La Morgia et al., 2018); LLMs may open a new perspective if it becomes possible to dispense with humans for this task.

2.2. The Emergence of LLMs: ChatGPT and DeepSeek

The launch of ChatGPT by OpenAI in November 2022 caused a convulsion that transcended the ICT field, bringing generative artificial intelligence within reach of people without specialized technical knowledge. Millions of users began interacting with AI in a simple manner, triggering a wave of changes and debates that affected society globally. Leading technology companies in Silicon Valley reacted quickly: Google launched Gemini, its advanced language model; Microsoft strengthened its commitment with multimillion-dollar investments in OpenAI; Meta developed its own language models, such as LLaMA, and offered them openly; X (formerly Twitter) presented Grok, a model focused on social interaction, among many others. Additionally, companies such as Amazon and Apple also intensified their AI efforts, integrating generative technologies into their service and device ecosystems. However, this boom was abruptly interrupted in early 2025 with the emergence of DeepSeek, a Chinese startup backed by a hedge fund. DeepSeek, a surprisingly economical and open-source alternative, not only challenged the dominance of OpenAI and other Western companies. DeepSeek altered almost all expectations in the AI sector, demonstrating that innovation is not limited to Silicon Valley and that the global artificial intelligence market is more dynamic and competitive than many anticipated.

Beyond the socioeconomic implications, ChatGPT and DeepSeek represent two complementary approaches within LLMs, technologies that have redefined natural language processing through the Transformer architecture (Vaswani et al., 2017). Both systems operate through sophisticated attention mechanisms that assign contextual relevance to each term, allowing for the identification of patterns and semantic relationships in large volumes of data, which, combined with Internet search systems, opens very promising information analysis expectations.

ChatGPT has consolidated itself as a benchmark in generating fluid and contextualized dialogues. Its effectiveness is based on a two-phase process: massive pre-training on multilingual corpora (books, articles, websites) and reinforcement learning with human feedback (RLHF) (Ouyang et al., 2022), where human adjusters rate responses to prioritize coherence and safety. This duality allows it to adapt to tasks as diverse as creative writing or technical assistance simulation, with an inherent risk: the generation of hallucinations (plausible but false statements) when extrapolating patterns from unverified data (Bender et al., 2021).

DeepSeek is an open-source LLM optimized for deep semantic analysis and misinformation detection. Although it shares the technical basis of the Transformer, its design incorporates techniques such as Retrieval-Augmented Generation (RAG) (Lewis et al., 2020), which links the model to external databases to verify claims in real time. Additionally, its specialized multilingual training (Spanish, Chinese, English) and computational efficiency position it as a scalable tool for processing massive data streams.

The introduction of DeepSeek as an open-source and free alternative to ChatGPT marks a turning point in the AI field, offering new possibilities for scientific research. While both models share significant strengths in improving efficiency and democratizing access, the differences in their transparency, cost, and accessibility have profound implications for innovation, ethics, and resource allocation. The transition of AI from an assistive tool to an active collaborator requires continuous adaptation of research practices (Kayaalp et al., 2025). Both models share the ability to perform deep linguistic analysis, identifying indicators of emotional manipulation, absence of sources, and internal contradictions, elements frequently associated with the dissemination of false information (Shu et al., 2017).

2.3. Misinformation Detection with LLMs: Advances and Perspectives

LLMs have transformed the field of misinformation detection. Pre-trained models such as BERT and RoBERTa had already established a solid foundation for text classification (Liu et al., 2019). However, current LLMs, based on Transformer architectures, offer superior contextual understanding and semantic reasoning capabilities, enabling a more adaptive approach to misinformation (Papageorgiou et al., 2025). A key contribution of LLMs is their application in few-shot fake news detection scenarios. This capability is crucial for quickly adapting to new misinformation narratives, as these models can generalize from a very small number of examples, surpassing the limitations of traditional supervised methods (Patel et al., 2025).

The integration of explainability techniques (Explainable AI) has become a fundamental pillar. Methodologies such as LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations) allow for breaking down the rationale behind a classification, identifying key words or phrases associated with false content (Patel et al., 2025). This is essential both for system auditing and for providing useful feedback to human verifiers. Recent research also points toward multimodal detection, where LLMs are combined with neural networks to process information from text, images, and videos. The construction of feature fusion modules allows for identifying subtle inconsistencies between different formats, a common characteristic in modern misinformation campaigns (Lu y Yao, 2025).

However, this potential coexists with significant challenges. LLMs are prone to hallucinations—the generation of plausible but false statements—which compromises their reliability as detectors (Pooley, 2024). There is also the risk of knowledge cannibalism: as AI-generated content floods the internet, future models could be trained on outputs from other models, degrading the quality of their knowledge base (Pooley, 2024). The detection of camouflaged misinformation, which mimics legitimate sources, requires models to focus on factual analysis rather than superficial stylistic patterns (García, 2024).

Overall, LLMs are not a single solution but powerful tools whose effectiveness depends on intelligent integration with external verification methods and a critical understanding of their limitations. ChatGPT and DeepSeek offer several promising capabilities, but the one affecting the present work consists of their ability to ‘read’ the web to process and ‘reason’ about its content. In this way, the user can quickly create a scraping tool without needing coding knowledge and benefiting from the language model for its analysis. The following section details the steps followed in this experiment.

3. Objectives

The primary objective of this article addresses the presence of major academic publishers on these channels and the possibility of detecting potential fake channels using ChatGPT and DeepSeek. To this end, we propose answering the following research questions:

1. Do fake channels impersonating the most important academic publishers exist on Telegram?
2. Could ChatGPT and DeepSeek serve to identify these channels?
3. What web sources do these LLMs use to answer the previous question?
4. Is there any bias in sources by country depending on the origin of each model?

4. Materials and Methods

The present study adopts a multiple case study design, following the methodological guidelines established by Yin (2018). According to this author, the case study constitutes empirical research that examines a contemporary phenomenon within its real context, being especially appropriate when the boundaries between the phenomenon and the context are not clearly evident. The choice of multiple cases (13 publishers and 37 associated channels) responds to the literal replication logic proposed by Yin, where each case serves as a 'replica' that allows confirming or refuting emerging patterns. Additionally, as Eisenhardt (1989) points out, research based on multiple cases is particularly suitable for novel thematic areas—as in this case—since it allows for generating empirically grounded theory from systematic comparison between cases. Below, the justification for the case study is presented, addressing its background, the purpose of its selection, and the units of analysis.

4.1. Case Background

The proliferation of fake channels on messaging platforms constitutes a phenomenon that has intensified in recent years, especially after the COVID-19 pandemic. Telegram presents structural characteristics that make it particularly vulnerable to identity impersonation. Unlike other platforms, Telegram has positioned itself as a service with minimal moderation, which facilitates the creation of channels that imitate legitimate organizations (Urman and Katz, 2022). The impact of these vulnerabilities in the realm of scientific communication is especially concerning. Academic identity impersonation scandals have shaken the publishing sector in recent years, with documented cases of fake authors, fraudulent acceptance letters, and use of artificial intelligence to fabricate data (Stockemer and Reidy, 2024). This erosion extends to the scientific domain when unverified channels disseminate information under the guise of recognized academic publishers.

Although Telegram has implemented a third-party verification system, its adoption by academic publishers has been virtually nonexistent. None of the publishers analyzed in this study had officially verified channels on the platform. This absence of official verification leaves a vacuum that malicious actors exploit through the use of names, logos, and descriptions that mimic legitimate organizations.

4.2. Purpose of Selection

Publisher selection criteria: The 13 major academic publishers were selected based on the number of journal titles indexed in SCImago Journal and Country Rank (query January 2025, N > 30k sources). The criterion of number of titles, rather than documents published, was deliberately adopted to avoid the bias that megajournals would introduce and to ensure representation of the publishing ecosystem in its diversity. The selected publishers (Elsevier, Springer, Wiley-Blackwell, Routledge, Oxford University Press, De Gruyter, Brill, Cambridge University Press, IEEE, Hindawi, World Scientific, Nature, and Thieme) represent the main actors in the sector and, therefore, the most likely targets for impersonation. The complete list with different variants can be found in Appendix I.

Justification for the Telegram platform: The choice of Telegram as the object of study responds to three converging factors. First, its growing use for the dissemination of academic and scientific content, documented in recent studies on misinformation ecosystems (Pietro et al., 2024). Second, its structural verification limitations, which contrast with more regulated platforms and generate specific vulnerabilities for institutional identity impersonation (Herrero and Castro, 2022). Third, the public accessibility of channel content through direct URLs (t.me/s/[channel]), which allows for analysis through LLMs with web browsing capability.

Justification for selected LLMs: As anticipated in the introduction, the selection of ChatGPT and DeepSeek as analysis tools responds to their representativeness within the current landscape of language models. ChatGPT, developed by OpenAI, maintains a dominant position in the Western market with a share exceeding 80% among generative AI chatbots, consolidating itself as the commercial benchmark for verification applications. DeepSeek represents a relevant methodological counterpoint: an open-source model developed under restrictions on access to advanced hardware that, nevertheless, has demonstrated competitive capabilities. The comparison between both models allows for evaluating whether differences in architecture, training, and orientation (commercial vs. open-source / USA vs. China) influence the ability to detect fraudulent channels.

4.3. Units of Analysis

Following the hierarchical structure recommended by Yin (2018) for multiple case studies, this study defines three levels of analysis:

Level	Unit of Analysis	N	Description
1	Academic publishers	13	Major publishers according to SCImago by number of titles
2	Telegram channels	37	Channels identified through publisher name search
3	LLM evaluations	74	ChatGPT (37) + DeepSeek (37)

Table 1 – Units of analysis

Variables collected for each channel: channel name, account (@username), associated publisher, number of followers, profile text, classification issued (REAL/FAKE/UNK) by each LLM, web sources cited by each LLM, geographical domain of sources, and finally reference labeling (ground truth) established by the researchers.

Temporal delimitation: The evaluations were conducted using ChatGPT-V4o and DeepSeek-V3 versions, between February 1 and 15, 2025, both with the web search function enabled.

Scope delimitation: Only public channels whose name, description, or content could generate confusion with official publishers were included. Private groups (not publicly accessible) and clearly parodic or satirical channels without impersonation intent were excluded.

4.4. Data Collection Procedure

The data collection procedure followed a standardized protocol to ensure replicability:

Channel identification: For each of the 13 publishers, a search was conducted on Telegram using the publisher's name. Telegram's search system displays a maximum of 10 results per query. All channels that could be confused at first glance with the official publisher were retained.

Data registration: For each identified channel, the name, account (@username), number of followers, and profile text were recorded in a structured dataset.

LLM evaluation: The following standardized prompt was sent to ChatGPT and DeepSeek for each channel:

> You are an expert in Telegram application channels. Could you indicate if the channel @[channel_name] on Telegram is an official channel of the publisher [publisher] or if it could be a fake channel? You can find the channel's content on the web https://t.me/s/[channel_name]. What facts do you base your assessment on to determine if it is fake or not?

The prompt was formulated in English to maximize both models' ability to access international web sources. Each evaluation was conducted in a new chat, without activating deep thinking and with the web search option enabled.

Response recording: The complete responses from each model were documented, including the classification issued and the web domains cited as verification sources.

Manual verification: The researchers established a ground truth classification through manual verification of each channel, consulting the official websites of the publishers, their verified profiles on other social networks, and the historical content of the channels.

5. Results

First, Figure 1 presents a ranking of publishers with the composition of journal titles by country. We find a strong predominance of the United States, the United Kingdom, and the Netherlands, in general, and of some countries in specific publishers such as Germany in Springer, de Gruyter, and Thieme, or Egypt in Hindawi.

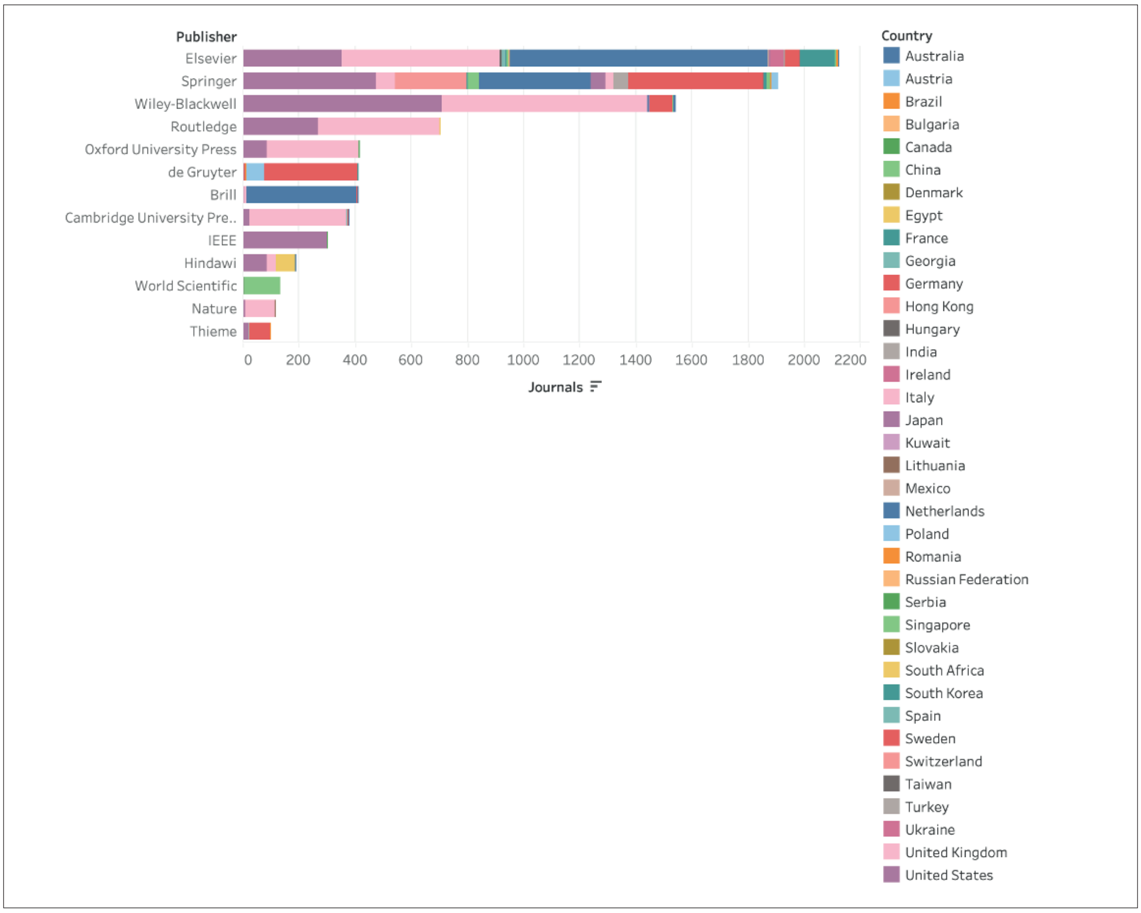

Figure 1. Volume of titles by country for each publisher.

5.1. Response Evaluation

It should be noted that in none of the 37 analyzed channels does the verification mark that Telegram places on official channels appear; very few of them include a URL, which is an essential element in verification, and the information published in the channels is observed to be quite heterogeneous. Something similar occurs with the number of followers and the number of publications in each channel, which are highly disparate. In the manual analysis of the channels, it was concluded that only 8 of 37 were real channels effectively linked to the publishers, representing 21.62% of the total. Figure 2 shows these results.

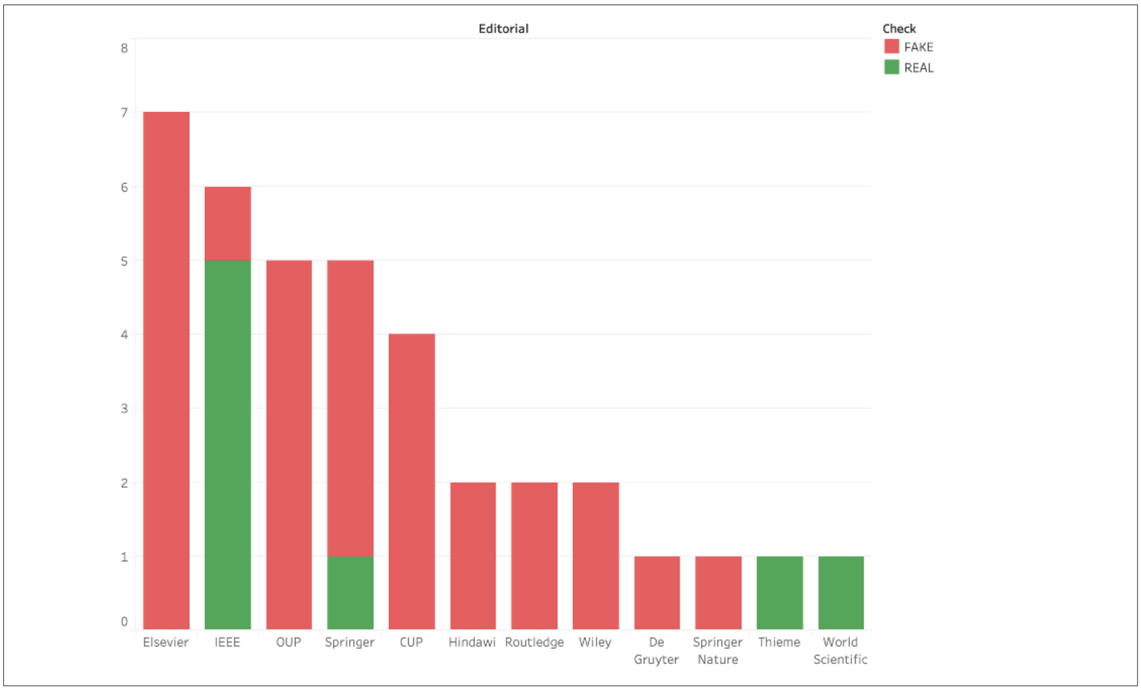

Figure 2. Relationship between real and fake channels by publisher

The analysis of Telegram channel content performed by the models reveals detailed conclusions about what these channels publish, which is fundamental for determining whether they are real or fake. Regarding the analysis and detection of fraudulent content, several channels are considered FAKE based on the type of services and language used, which is inconsistent with the practices of prestigious publishers, such as repeated advertisements for article submission, publication fees, and fast submission deadlines. It is noteworthy that unusual claims appear, such as review times and free proofreading and indexing in journals for a fee, practices associated with predatory journals.

The models show accuracy in detecting publications with fraudulent content and in locating claims contradictory to the publishers' own marketing policies, with books appearing in different formats without providing clear information about copyright or licenses. The models also detect incongruent presences, such as the distribution of Cambridge University Press materials despite bearing the Oxford University Press name.

Regarding content consistent with official or legitimate affiliation, in some channels, mainly those affiliated with IEEE, content is located that supports (or at least does not refute) their local or thematic legitimacy. The channel content analysis demonstrates that most FAKE channels use content (free books, promises of rapid publication) as bait to attract users, while channels classified as REAL or legitimately affiliated (mainly IEEE) are restricted to strictly professional, technical content linked to official platforms of the organization. The models also take into account, though to a lesser extent, the fact of channel inactivity or the sparse publications of some.

In the manual review and in the model responses, it is observed that in FAKE channels there is an intent to impersonate, using different derivations in the channel name and its identification, with clear intention of impersonating the publisher, in some cases for the free dissemination of publications that are marketed on official websites. Regarding users and the number of publications, numerous channels have few publications and have been inactive for years.

It is also observed that most of those corresponding to IEEE are real. This is due to the fact that IEEE is a professional association in addition to being a publisher; these channels dedicate their publications to different matters, and although there are references and links to publications, their creation and use do not respond exclusively to editorial purposes.

Similarly, there is a small group of small publishers that use the channel as a means of disseminating information about their publications and various activities, but the fact that they have not managed to obtain Telegram's verification checkmark could be an indication that the channel is not a priority in their dissemination and marketing policies.

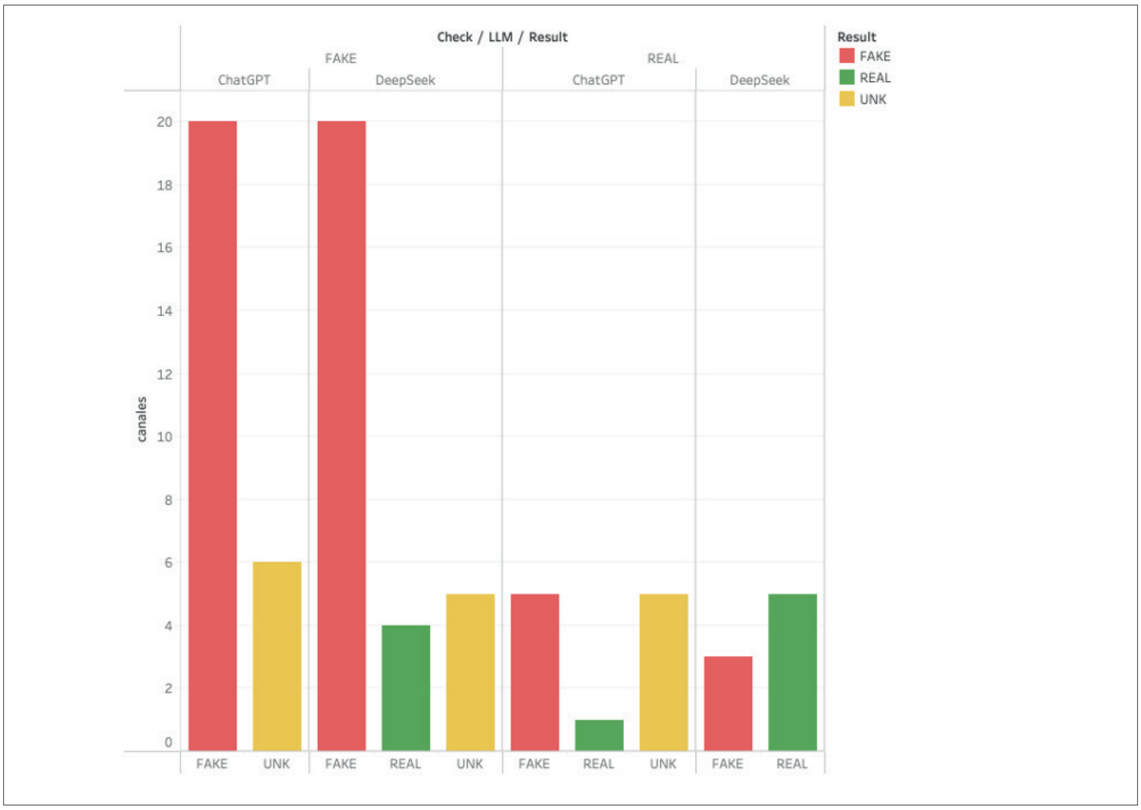

Figure 3. Relationship between real and fake channels according to model consideration

Figure 3 shows a high level of accuracy by both models in determining the falsity of FAKE channels. In the case of ChatGPT, it does not consider any of the fake ones as real, considering as doubtful a group similar to that considered by DeepSeek as such. The group of FAKEs that DeepSeek considers real stands out, suggesting that the referral from content to legitimate domains and official institutions may have caused them to be considered real.

In the case of the response to real channels, it is observed that DeepSeek divides its responses between real and fake, not considering any as doubtful, while ChatGPT limits the number it considers real to one, considering a similar group as doubtful or fake. This shows that the models tend to fail in identifying real channels due to dependence on global verification criteria (blue badge and corporate links), ignoring the legitimacy of the content or regional affiliation.

5.2. Referenced Sites

In the dataset, we can find rankings of the most-used domains by each model. There is a total of 217 websites that were cited a total of 507 times. ChatGPT made more intensive use of references, a total of 319 versus 188 from DeepSeek. As the number of sites is very large, Table 2 shows only the most frequent for each LLM.

ChatGPT				Deepseek			
Site	**Group**	**Country**	**#**	**Site**	**Group**	**Country**	**#**
t.me	Telegram	AE	35	t.me	Telegram	AE	33
facebook.com	Social networks	US	15	keepersecurity.com	Ciberseguridad	US	11
telemetr.io	Telegram	US	9	telegram.org	Telegram	AE	9
youtube.com	Social networks	US	9	infostealers.com	Ciberseguridad	US	7
reddit.com	Social networks	US	9	lifelock.norton.com	Ciberseguridad	US	6

Table 2. Top 5 cited sites

To analyze all sites, we grouped them into categories and also included the reference country. In some cases, this was straightforward, but in others, it was not. In addition to reviewing the websites, we used the Whois service and even asked the LLMs themselves. In this way, we obtain the ranking in Table 3, where we have each group and the cumulative frequency in which they appear (ChatGPT + DeepSeek). The main group consists of the different variants of the Telegram service. It is reasonable that this is the case since in the prompt itself we asked the models to analyze this service. Second, we have social network services in general, some as well-known as Facebook, YouTube, or Reddit, but there are also others less prominent. Within Top Publishers, we include the websites of the publishers under study, and within Publishers, the rest.

Group	Frequency
Telegram	117
Social networks	64
Top publishers	52
Cybersecurity	50
Repositories	41
Publishers	39
Universities	37
Media	24
Governments	22
Digital marketing	17
Academic black hat	16
Crypto	15
Educational blog	7
Academic journals	3
Fake news	2
Marketplace	1

Table 3 – Site frequency by group

It is important to highlight the Cybersecurity group since there was a large number of sites related to this topic, a priori unexpected, and the same occurred with everything related to the Crypto world. Of the rest, perhaps it is necessary to highlight what we have called Academic black hat, which is nothing more than websites where access to copyrighted material is facilitated in a clear (or disguised) violation thereof.

In Figure 4, we can appreciate the biases of each model with each group. Clearly, Telegram appears in both; however, Cybersecurity (and Crypto to a lesser extent) stands out in DeepSeek. ChatGPT, for its part, seems to use more mainstream sites such as social networks themselves, universities, or government sites. Publishers, Top Publishers, and Repositories appear referenced by both models. It is worth noting that Academic black hat is mentioned by both models, although ChatGPT does so to a greater extent.

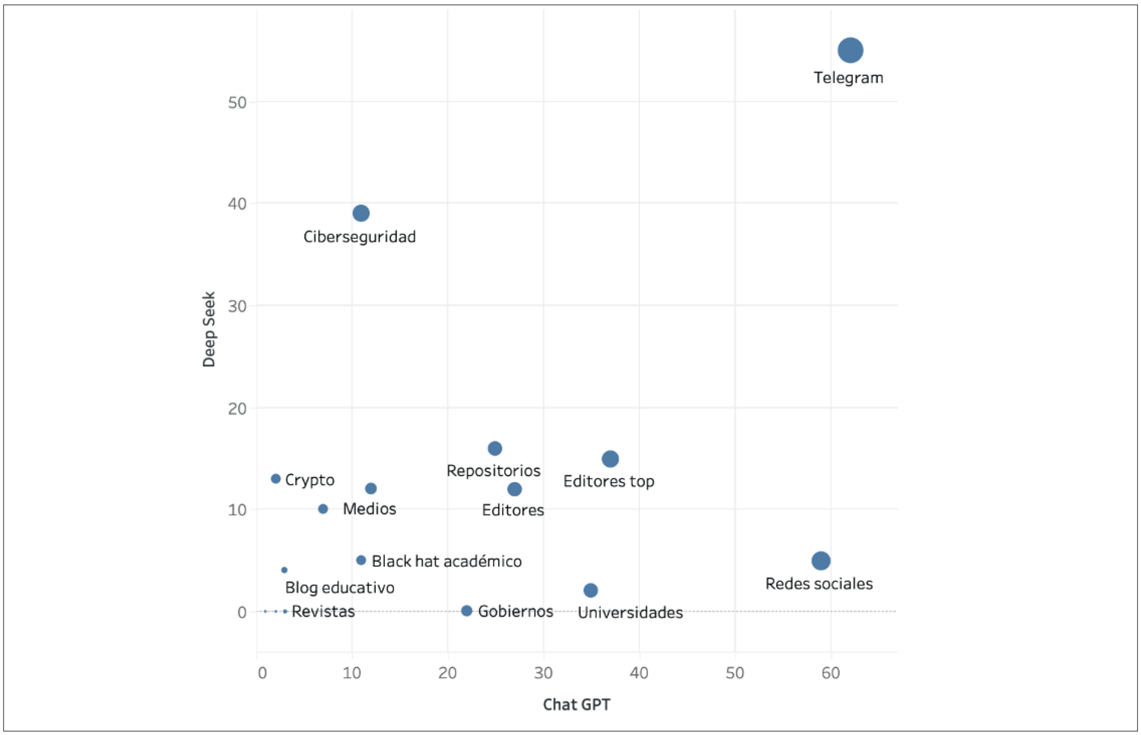

Figure 4. Comparison of sites by model

But what is most striking is the provenance of media by country. In this case, no notable bias is appreciated. Figure 5 shows countries with two or more appearances. The predominant country is the United States, for both the American and Chinese models. In second place, we have the United Arab Emirates since it is the headquarters of the Telegram service, and a little further behind the United Kingdom and Germany. Up to this point, total dominance of Western web space. In fifth and sixth place, we have two non-Western actors: Russia and India. It is striking that Russia appears biased toward ChatGPT while India is biased toward DeepSeek, where it was especially used within the cybersecurity topic.

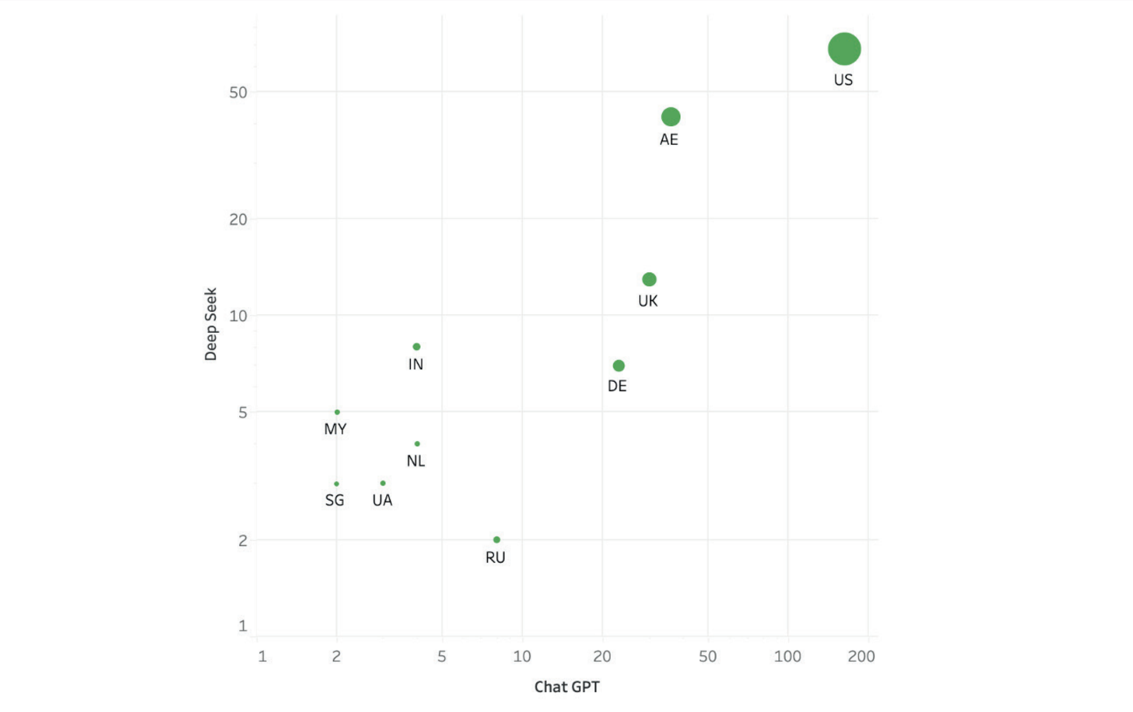

Figure 5. Distribution of countries by model

Finally, we should note that in the entire dataset there is only one Chinese site, something truly curious.

6. Discussion

The present research confirms the massive proliferation of unofficial channels that impersonate the identity of major academic publishers on Telegram. The data reveal that 78.38% of the analyzed channels present fraudulent characteristics or unauthorized practices, constituting a parallel ecosystem that operates outside the official channels of scientific communication. This finding is consistent with previous research that has documented the existence of an extensive network of fake and clone channels on the platform (La Morgia et al. 2021, 2023), and establishes that identity impersonation or the operation of unofficial channels is the norm, not the exception, in this ecosystem.

This phenomenon cannot be dissociated from the broader context of Western editorial hegemony identified in our Figure 1, where the United States, the United Kingdom, and the Netherlands concentrate the majority of production. This concentration inevitably creates economic, linguistic, and geopolitical barriers to access, which in turn generate a breeding ground for informal markets that promise to circumvent these restrictions. The recurring appearance in our sources of categories such as 'academic black hat' corroborates the existence of an organized digital infrastructure that sustains this gray economy, a phenomenon that has also been identified in the context of academic editorial fraud (Stockemer and Reidy, 2024).

Regarding the fraud mechanisms identified, FAKE channels use specific tactics inconsistent with legitimate academic communication. First, fraudulent promotion, characterized by informal and promotional language, with unusual claims such as extremely fast publication deadlines (2-3 weeks) and the mention of high fees ($1200 USD), which align with the characteristics of predatory journals or scams. Second, unauthorized distribution and piracy: channels related to book publishers (OUP, Springer) offer free access to materials that the publisher normally markets, which is atypical for a legitimate publisher. These patterns coincide with those described by Herasimenka et al. (2023) in their analysis of minimally moderated platforms, where the ease of channel creation and the absence of preventive verification facilitate the proliferation of misleading content. The most common characteristic of unofficial channels is the absence of Telegram's blue verification badge, which publishers of the caliber we are studying should display if the channel were official.

The large presence of FAKE channels, which often combine pirated content distribution with suspicious publication services, represents a significant risk to academic integrity and publisher brands. This finding ratifies that the possibility of generating any public channel, with any name, since verification is only provided a posteriori and only if the corporation or entity requests it, opens a notable space for fraud possibilities. It is striking that academic publishers do not seem to show special interest in this channel which, well exploited and correctly verified, could constitute a robust means of dissemination for them. This institutional neglect contrasts with the growing relevance of Telegram as an information dissemination platform (Willaert, 2023; Sánchez and Martos, 2020).

Regarding the suitability of LLM models as analysis tools, our results present a nuanced picture. The significant agreement between both models in identifying clearly fraudulent channels suggests that these tools can effectively detect common impersonation patterns, which is consistent with recent research demonstrating the ability of LLMs to identify misleading content through contextual analysis (Chen and Shu, 2024; Papageorgiou et al. 2025). However, the notable discrepancies in the verification of real channels reveal deep structural limitations. DeepSeek demonstrates a marked tendency toward what we might call a 'contextual criterion,' showing greater willingness to validate channels that present coherent content and local collaborations, even in the absence of formal verification. In contrast, ChatGPT operates under a 'strict verification' paradigm, requiring explicit evidence of institutional affiliation and showing considerably greater caution.

This divergence in evaluation criteria has important implications. The models can be fooled by the professional appearance of content or by the use of technical terms (such as Scopus, Nature, etc.), without being able to validate critical indicators of authenticity. This limitation connects with warnings about LLM hallucinations—the generation of plausible but false statements—that compromise their reliability as autonomous detectors (Bender et al., 2021; Pooley, 2024). The results reinforce the need to consider these tools as complementary support to expert judgment, not as substitutes for it, as suggested by Patel et al. (2025) in their proposal for misinformation detection systems.

The examination of web sources consulted by the models reveals notably different knowledge architectures. Beyond the expected predominance of domains associated with Telegram, the cybersecurity field emerges with unusual force in the case of DeepSeek, while ChatGPT shows preference for institutional sources and conventional social networks. This disparity suggests that each model constructs its interpretive framework on substantially different web search agents, which necessarily conditions their evaluations. DeepSeek, by relying on resources specialized in digital security, seems to develop an acute sensitivity toward fraud and impersonation patterns, an approach reminiscent of pattern analysis-based detection techniques described by Shu et al. (2017). ChatGPT, with its broader and more conventional base, prioritizes formal institutional verification. Both approaches present complementary advantages, but their disconnect largely explains the observed discrepancies in classifications.

The absolute predominance of Western sources in both models reflects the still-prevailing hegemony of the so-called developed countries in the global architecture of the internet, a bias that has been documented in previous studies on the geographical distribution of online knowledge (Allcott and Gentzkow, 2017). However, the differential affinities—DeepSeek with Indian and South Asian sources, ChatGPT with Russian sources—suggest that source search agents are not completely predetermined. The particularly eloquent case of the near absence of Chinese sources, despite DeepSeek's origin, merits additional investigation. This finding connects with observations by Urman and Katz (2022) about how network structures on Telegram can replicate broader ideological and geographical divisions.

Finally, our results have implications for understanding the broader phenomenon of information disorder described by Wardle and Derakhshan (2017). Fake Telegram channels that impersonate academic publishers do not constitute solely a problem of intellectual property or commercial fraud but rather erode trust in scientific communication institutions. In a context where scientific misinformation has demonstrated serious consequences for public health and democratic debate (Díez-Garrido et al., 2021; Prieto-Campo et al., 2024), the proliferation of these channels represents a structural threat requiring coordinated responses from both technological platforms and academic publishers themselves.

7. Conclusions

This work reveals that, in the Telegram ecosystem, the presence of major academic publishers is profoundly distorted by an overwhelming majority of unofficial channels that impersonate their identity. From the analysis of 37 channels associated with 13 leading publishers, it was found that 78.38% of the channels are fraudulent or lack verifiable links to the corresponding publisher, while only 21.62% can be considered real or legitimately affiliated. This situation configures an environment structurally prone to misinformation and intellectual property rights violations.

Regarding the first research question, our results confirm the existence of an extensive and organized network of unofficial channels that appropriate names, logos, and descriptions belonging to academic publishers. These channels combine unauthorized content distribution (especially books) with editorial service offers of dubious legitimacy, aligned with practices characteristic of predatory journals. The generalized absence of official Telegram verification and the limited active presence of publishers on the platform favor these fraudulent channels becoming, de facto, visible references for many users.

Regarding the second research question, the results show that ChatGPT and DeepSeek are useful tools for the initial mapping and characterization of this fraudulent ecosystem, especially in identifying clearly FAKE channels. Both models frequently agree on the detection of fraud patterns. However, they present important limitations in validating real channels, where they tend to overreact to the absence of strong institutional signals (verified channels, corporate web links) and to undervalue legitimate content with local or regional visibility. The difference between DeepSeek's more 'contextual' approach and ChatGPT's greater demand for 'formal verification' suggests that these models operate under partially divergent evaluation logics, which reinforces the need to use LLMs as complementary support, and not as a substitute, for expert human judgment.

Regarding the third and fourth questions, the thematic content of consulted sources reveals that knowledge construction in these systems is mediated by specific documentary architectures that reflect differentiated thematic priorities and alignments. DeepSeek's bias toward cybersecurity and ChatGPT's 'institutionalism' (universities, governments, publishers) do not appear to constitute mere technical differences but complementary visions of a complex phenomenon. However, this difference is not clearly verified when we look at the origin of sources. There is a bias toward Western sources, which seems to indicate that the training of both models has been based on not very different datasets. The presence of Chinese sources is almost nil (0.2%), even in the case of DeepSeek, a model that at times gives the impression of being Indian or from Southeast Asia (Malaysia and Singapore). Overall, the results suggest that the differences between both LLMs are explained more by the logic of their search agents and the thematic prioritization of their sources than by the country of origin of each model.

As future lines of work, this study opens several avenues of interest. On the methodological level, it is pertinent to incorporate other relevant LLMs. Among them, currently noteworthy, in our view, are Claude (Anthropic), Gemini (Google), Qwen (Alibaba), the controversial Grok (X), and the newcomer Kimi K2. With them, we can evaluate whether the differences observed in this work hold across a broader spectrum of models. On the applied level, it would be valuable to extend the approach to other types of scientific and political misinformation present on Telegram, including the detection of fake news and conspiracy narratives. The progressive integration of massive data analysis capabilities by LLMs offers an opportunity to design hybrid systems in which computational scale and human judgment mutually reinforce each other in protecting the integrity of scientific communication.

Acknowledgments

This paper has received funding from the Knowledge Generation Projects 2023 program of the Spanish Ministry of Science, Innovation and Universities through the project 'Artificial Intelligence in Europe: Rise or Decline?' (PID2023-149646NB-I00).

8. Bibliography

Abu-Ayfah, Zainab A. 2020. "Telegram App in learning English: EFL students' perceptions". *English Language Teaching*, 13(1): 51-62. https://doi.org/10.5539/elt.v13n1p51

Allcott, Hunt, & Matthew Gentzkow. 2017. "Social media and fake news in the 2016 election". *Journal of Economic Perspectives*, 31(2): 211-36. https://doi.org/10.1257/jep.31.2.211

Bender, Emily M., Timnit Gebru, Angelina McMillan-Major, & Shmargaret Shmitchell. 2021. "On the dangers of stochastic parrots: can language models be too big?". In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 610-623. https://doi.org/10.1145/3442188.3445922

Carew, Sinéad, Amanda Cooper, & Ankur Banerjee. 2025. "DeepSeek sparks global AI selloff; Nvidia loses about $593 Billion of value". *Reuters*, January 27. https://www.reuters.com/technology/chinas-deepseek-sets-off-ai-market-rout-2025-01-27

Chen, Caiwei. 2025. "How a top Chinese AI model overcame US sanctions". *MIT Technology Review*, January 24. https://www.technologyreview.com/2025/01/24/1110526/china-deepseek-top-ai-despite-sanctions

Chen, Canyu, & Kai Shu. 2024. Combating misinformation in the age of LLMs: Opportunities and challenges. *AI Magazine*, 45(3): 313-331. https://doi.org/10.1002/aaai.12188

Cho, Hichang, Sungjong Roh, & Byungho Park. 2019. "Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings". *Computers in Human Behavior*, 101. https://doi.org/10.1016/j.chb.2019.07.001

Cisternas-Osorio, Rodrigo, Alberto J. López-Navarrete, Margarita Cabrera-Méndez, & Rebeca Díez-Somavilla. 2022. "Telegram para el ejercicio de la comunicación interna: Análisis de su uso en universidades hispanohablantes". *Fonseca, Journal of Communication*, 25: 77-93. https://doi.org/10.14201/fjc.29750

Dargahi Nobari, Arash, Negar Reshadatmand, & Mahmood Neshati. 2017. "Analysis of Telegram, an instant messaging service". In *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, 2035-2038. https://doi.org/10.1145/3132847.3133132

Dargahi Nobari, Arash, Malikeh Haj Khan Mirzaye Sarraf, Mahmood Neshati, & Farnaz Erfanian Daneshvar. 2021. "Characteristics of viral messages on Telegram; The world's largest hybrid public and private Messenger". *Expert Systems with Applications*, 168: 114303. https://doi.org/10.1016/j.eswa.2020.114303

Díez-Garrido, María, Covadonga Renedo Farpón, & Lorena Cano-Orón. 2021. "La desinformación en las redes de mensajería instantánea. Estudio de las fake news en los canales relacionados con la ultraderecha española en Telegram". *Miguel Hernández Communication Journal*, 12(2): 467-89. https://doi.org/10.21134/mhjournal.v12i.1292

Durov, Pavel. 2024. Canal Telegram Pavel Durov, 6 de septiembre. https://t.me/PavelDurovs/284

Eisenhardt, Kathleen M. 1989. "Building theories from case study research". *Academy of Management Review* 14(4): 532-50. https://doi.org/10.2307/258557

Flores-Vivar, Jesús Miguel, & Francisco José García-Peñalvo. 2023. "Reflexiones sobre la ética, potencialidades y retos de la Inteligencia Artificial en el marco de la Educación de Calidad (ODS4)". *Comunicar*, 31(74): 37-47. https://doi.org/10.3916/C74-2023-03

García-Marín, David. 2024. "Periodismo contra la desinformación. Proceso y estructura de las verificaciones en el fact-checking". *Infonomy*, 2(2): e24026. https://doi.org/10.3145/infonomy.24.026

Ghaffari, Mohtasham, Sakineh Rakhshanderou, Yadollah Mehrabi, & Afsson Tizvir. 2017. "Using social network of Telegram for education on continued breastfeeding and complementary feeding of children among mothers: A successful experience from Iran". *International Journal of Pediatrics*, 5(7): 5275-86. https://doi.org/10.22038/ijp.2017.22849.1915

Gregorio, Jesús, Alfredo Gardel, & Bernardo Alarcos. 2017. "Forensic analysis of Telegram messenger for Windows phone". *Digital Investigation*, 22: 88-106. https://doi.org/10.1016/j.diin.2017.07.004

Gregorio, Jesús. 2000. *Contribuciones al análisis forense de evidencias digitales procedentes de aplicaciones de mensajería instantánea*. Tesis doctoral, Universidad de Alcalá. https://ebuah.uah.es/dspace/handle/10017/50754?locale-attribute=es

Herasimenka, Aliaksandr, Jonathan Bright, Aleksi Knuutila, & Philip N. Howard. 2023. "Misinformation and professional news on largely unmoderated platforms: The case of Telegram". *Journal of Information Technology & Politics*, 20 (2): 198-212. https://doi.org/10.1080/19331681.2022.2076272

Herrero-Solana, Víctor, & Carlos Castro-Castro. 2022. "Telegram channels and bots: A ranking of media outlets based in Spain". *Societies*, 12(6): 164. https://doi.org/10.3390/soc12060164

Jakobsen, Jakob Bjerre. 2015. *A practical cryptanalysis of the Telegram messaging protocol*. Master's thesis, Aarhus University. https://enos.itcollege.ee/~edmund/materials/Telegram/A-practical-cryptanalysis-of-the-Telegram-messaging-protocol_master-thesis.pdf

Jalilvand, Asal, & Mahmood Neshati. 2020. "Channel retrieval: Finding relevant broadcasters on Telegram". *Social Network Analysis and Mining*, 10(1). https://doi.org/10.1007/s13278-020-0629-z

Kayaalp, Mahmut E., Robert Prill, Erdem A. Sezgin, Ting Cong, Aleksandra Królikowska, & Michael T. Hirschmann. 2025. "DeepSeek versus ChatGPT: Multimodal artificial intelligence revolutionizing scientific discovery. From language editing to autonomous content generation. Redefining innovation in research and practice". *Knee Surgery, Sports Traumatology, Arthroscopy*, 33(5), 1553-1556. https://doi.org/10.1002/ksa.12628

Kitsa, Mariana. 2023. "Telegram news channels: Overview of audience preferences and their implications". *Social Journal Studies*, 12(6): 354-69.

La Morgia, Massimo, Alessandro Mei, Alberto Maria Mongardini, & Jie Wu. 2018. "Pretending to be a VIP! Characterization and detection of fake and clone channels on Telegram". *ACM Transactions on the Web*, 12(4). https://dl.acm.org/doi/pdf/10.1145/3705014

La Morgia, Massimo, Alessandro Mei, Alberto Maria Mongardini, & Jie Wu. 2021. "Uncovering the Dark Side of Telegram: Fakes, clones, scams, and conspiracy movements". arXiv preprint arXiv:2111.13530. https://arxiv.org/pdf/2111.13530

La Morgia, Martina, Alessandro Mei, Alberto Maria Mongardini, & Jie Wu. 2023. "It's a trap! Detection and analysis of fake channels on Telegram". In 2023 *IEEE International Conference on Web Services (ICWS)*, 97-104. IEEE. https://doi.org/10.1109/ICWS60048.2023.00026

Lewis, Patrick, Ethan Perez, Aleksandra Piktus, Fabio Petroni, Vladimir Karpukhin, Naman Goyal, Heinrich Küttler, et al. 2020. "Retrieval-augmented generation for knowledge-intensive NLP tasks". *Advances in Neural Information Processing Systems*, 33: 9459-9474.

Liu, Yinhan, Myle Ott, Naman Goyal, Jingfei Du, Mandar Joshi, Danqi Chen, Omer Levy, Mike Lewis, Luke Zettlemoyer, & Veselin Stoyanov. 2019. "RoBERTa: A Robustly Optimized BERT Pretraining Approach". *arXiv*. Preprint submitted July 26. https://arxiv.org/abs/1907.11692

López-Tárraga, Ana Belén. 2020."Comunicación de crisis y ayuntamientos: El papel de Telegram durante la crisis sanitaria de la Covid-19". *RAEIC: Revista de la Asociación Española de Investigación de la Comunicación*, 7(14): 104-26. https://doi.org/10.24137/raeic.7.14.5

Lu, Ying & Naiwei Yao. 2025. "A fake news detection model using the integration of residual networks and attention mechanisms". *Scientific Reports*, 15: 20544. https://doi.org/10.1038/s41598-025-05702-w

Martos Moreno, Javier, & Hada M. Sánchez Gonzales. 2024. "Consumo incidental de noticias en Telegram". *Estudios sobre el Mensaje Periodístico*, 30(1): 167-176. https://doi.org/10.5209/esmp.92127

Mohammed, Ibrahim A., Ibrahim I. Kuta, Oluwole C. Falode, & Ahmed Bello. 2024. "Comparative performance of undergraduate students in micro teaching using Telegram and WhatsApp in collaborative learning settings". *Journal of Mathematics and Science Teacher*, 4(2). https://doi.org/10.29333/mathsciteacher/14411

Ouyang, Long, Jeff Wu, Xu Jiang, Diogo Almeida, Carroll L. Wainwright, Pamela Mishkin, Chong Zhang, et al. 2022."Training language models to follow Instructions with human feedback". *Advances in Neural Information Processing Systems*, 35: 27730–44.

Papageorgiou, Eleftheria, Iraklis Varlamis, & Christos Chronis. "Harnessing Large Language Models and deep neural networks for fake news detection". *Information*, 16(4): 297. https://doi.org/10.3390/info16040297

Patel, Jainee, Chintan M. Bhatt, Himani Trivedi, Thanh Thi Nguyen, Kadi Sarva Vishwavidyalaya. 2025. "Misinformation detection using large Language models with explainability." In *Proceedings of the 8th International Conference on Algorithms, Computing and Artificial Intelligence*. https://arxiv.org/pdf/2510.18918

Prieto-Campo, Álvaro, Olalla Vázquez-Cancela, Fátima Roque, María-Teresa Herdeiro, Adolfo Figueiras, & Maruxa Zapata-Cachafeiro. 2024. "Unmasking vaccine hesitancy and refusal: A deep dive into anti-vaxxer perspectives on Covid-19 in Spain". *BMC Public Health*, 24(1751). https://doi.org/10.1186/s12889-024-18864-5

Pooley, Jeff. 2024. "Publicación en Large Language Model (LLM)". *SciELO in Perspective* (blog), 19 de enero. https://blog.scielo.org/es/2024/01/19/publicacion-en-llm

Sánchez Gonzales, Hada M., & Juan Martos Moreno. 2020. "Telegram como herramienta para periodistas: Percepción y uso". *Revista de Comunicación* 19(2): 245-61. https://doi.org/10.26441/RC19.2-2020-A14

Sedano Amundarain, Jon, & María Bella Palomo Torres. 2018. "Aproximación metodológica al impacto de WhatsApp y Telegram en las redacciones". *Hipertext.net*, 16. https://doi.org/10.31009/hipertext.net.2018.i16.10

Shu, Kai, Amy Sliva, Suhang Wang, Jiliang Tang, & Huan Liu. 2017. "Fake news detection on social media: A data mining perspective". *ACM SIGKDD Explorations Newsletter*, 19(1): 22-36.

StatCounter. 2025. "Leading AI chatbots on desktop devices worldwide between March and October 2025, by share of web referrals". Chart, 9 de noviembre de 2025. En *Statista*. https://www.statista.com/statistics/1625095/desktop-ai-chatbots-market-share

Steblyna, Nataliia O. 2024. "Digital media environment in wartime. Russian invasion coverage in Ukrainian professional and amateur news media". *Horyzonty Polityki*, 15(51): 99-119. https://doi.org/10.35765/hp.2484

Stockemer, Daniel, & Theresa Reidy. 2024. "Academic misconduct, fake authorship letters, cyber fraud: Evidence from the International Political Science Review". *Learned Publishing*, 37(1): 39-43. https://doi.org/10.1002/leap.1587

Sušánka, Tomáš, & Jozef Kokeš. 2017. "Security analysis of the Telegram IM". In *Proceedings of the 1st Reversing and Offensive-Oriented Trends Symposium*, 1-8. https://doi.org/10.1145/3150376.3150382

Telegram. "Mensajes por estrellas, regalos fijados, plataforma de verificación 2.0 y más". *Telegram*,12. https://telegram.org/blog/star-messages-gateway-2-0-and-more/es

Thorp, H. Holden. 2023. "ChatGPT is fun, but not an author". *Science*, 379(6630): 313. https://doi.org/10.1126/science.adg7879

Urman, Aleksandra, & Stefan Katz. 2022. "What they do in the shadows: Examining the far-right networks on Telegram". *Information, Communication & Society*, 25(7): 904-23. https://doi.org/10.1080/1369118X.2020.1803946

Vaswani, Ashish, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Łukasz Kaiser, & Illia Polosukhin. 2017. "Attention is all you need". *Advances in Neural Information Processing Systems*, 30.

Wardle, Claire, & Hossein Derakhshan. 2017. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking*. Strasbourg: Council of Europe.

Willaert, Tom. 2023. A computational analysis of Telegram's narrative affordances. *Plos one*, 18(11), e0293508. https://doi.org/10.1371/journal.pone.0293508

Yin, Robert K. 2018. *Case study research and applications: Design and methods*. 6th ed. Los Angeles: SAGE Publications.

9. Appendix I

Publishers with their variant names

Editorial	Variants
Elsevier	Elsevier; Elsevier B.V. ; Elsevier (Singapore) Pte Ltd; Elsevier Editora Ltda; Elsevier Espana; Elsevier Espana S.L.U; Elsevier GmbH; Elsevier Inc.; Elsevier Ireland Ltd; Elsevier Ltd; Elsevier Masson s.r.l.; Elsevier Science; Elsevier Science & Technology; Elsevier Science B.V.; Elsevier Taiwan LLC; Elsevier USA; Reed Elsevier India Pvt. Ltd.; Reed-Elsevier (India) Private Limited
Springer	Springer; Springer Berlin; Springer Boston; Springer China; Springer Fachmedien Wiesbaden GmbH; Springer Gabler; Springer GmbH & Co, Auslieferungs-Gesellschaf; Springer Healthcare; Springer Heidelberg; Springer India; Springer International Publishing; Springer International Publishing AG; Springer Japan; Springer London; Springer Medizin; Springer Nature; Springer Netherlands; Springer New York; Springer Paris; Springer Publishing Company; Springer Science + Business Media; Springer Science and Business Media B.V.; Springer Science and Business Media Deutschland GmbH; Springer Science and Business Media, LLC; Springer Singapore; Springer US; Springer Verlag; Springer Vieweg; Springer-Verlag GmbH and Co. KG; Springer-Verlag Italia s.r.l.; Springer-Verlag Wien; SpringerOpen;
Wiley-Blackwell	John Wiley & Sons Inc; John Wiley and Sons Inc; John Wiley and Sons Ltd; Wiley-Blackwell; Wiley-Blackwell for the International Association for the Study of Obesity; Wiley-Blackwell Publishing Ltd; Wiley-Liss Inc.; Wiley-VCH Verlag;
Routledge	Routledge; Brunner - Routledge (US); Routledge, Taylor & Francis Group
Oxford University Press	Oxford University Press
De Gruyter	de Gruyter; De Gruyter Mouton; De Gruyter Oldenbourg; De Gruyter Open Ltd.; De Gruyter Saur; Walter de Gruyter; Walter de Gruyter GmbH; Walter de Gruyter GmbH & Co. KG
Brill	Brill Academic Publishers; Brill Nijhoff; Brill Schoningh; Brill: Rodopi
Cambridge University Press	Cambridge University Press
IEEE	IEEE Advancing Technology for Humanity; IEEE Canada; IEEE Circuits and Systems Society; IEEE Communications Society; IEEE Computational Intelligence Society; IEEE Computer Society; IEEE CONTROL SYSTEMS SOCIETY; IEEE Education Society; IEEE Electromagnetic Compatibility Society; IEEE Electron Devices Society; IEEE Industrial Electronics Society; IEEE Power Electronics Society; IEEE Systems, Man, and Cybernetics Society; Institute of Electrical and Electronics Engineers Inc.
Hindawi	Hindawi; Hindawi Limited; Hindawi Publishing Corporation; Wiley-Hindawi
World Scientific	World Scientific; World Scientific Publishing Co. Pte Ltd; World Scientific Publishing Co., Inc.
Nature	Nature Partner Journals; Nature Publishing Group; Nature Research; Nature Research Centre
Thieme	Thieme; Georg Thieme Verlag; Thieme Medical Publishers; Thieme Medical Publishers, Inc.; Thieme Publishers Rio

10. Apendix II

Channel model conclusions and manual review

Canal	Editorial	DeepSeek	ChatGPT	Check
@ScopusElsevier	Elsevier	FAKE	FAKE	FAKE
@scopusservices	Elsevier	FAKE	FAKE	FAKE
@ElsevierCentralAsia	Elsevier	REAL	UNK	FAKE
@Elsevierscienceuzbekistan	Elsevier	FAKE	FAKE	FAKE
@clinicalkey	Elsevier	FAKE	UNK	FAKE
@elsevier_iran	Elsevier	REAL	UNK	FAKE
@elseviereducatiRealn	Elsevier	UNK	UNK	FAKE
@springer_uzb	Springer	FAKE	FAKE	FAKE
@NatureClimateTelegram	Springer	FAKE	UNK	REAL
@MasterTez	Springer	FAKE	FAKE	FAKE
@TAQUspringer	Springer	FAKE	FAKE	FAKE
@SPBooksMed	Springer	FAKE	FAKE	FAKE
@wileyrus	Wiley	REAL	FAKE	FAKE
@wiley_uz	Wiley	UNK	FAKE	FAKE
@routledgebooks	Routledge	UNK	UNK	FAKE
@routledge_bobil	Routledge	FAKE	FAKE	FAKE
@oupbooks	OUP	FAKE	FAKE	FAKE
@oxford_ielts_grammar_booksN1	OUP	FAKE	FAKE	FAKE
@oxford_university_press_bot	OUP	FAKE	FAKE	FAKE
@studycollegeTt	OUP	FAKE	FAKE	FAKE
@edupressUzbekistan	OUP	FAKE	UNK	FAKE
@degruyter	De Gruyter	UNK	UNK	FAKE
@cambridgeuni	CUP	FAKE	FAKE	FAKE
@cambridge_university_press_ielts	CUP	UNK	FAKE	FAKE
@cambridgeUniversityPresss	CUP	FAKE	FAKE	FAKE
@Cambridge_practice_discussion	CUP	FAKE	FAKE	FAKE
@ieeear	IEEE	FAKE	UNK	REAL
@aetel	IEEE/UPM	FAKE	FAKE	REAL
@IEEEbot	IEEE/UGR	FAKE	FAKE	FAKE
@ieeesiberia	IEEE	REAL	UNK	REAL
@IEEEIranSection	IEEE	REAL	REAL	REAL
@IEEESmartGrid	IEEE	REAL	UNK	REAL
@hindawi_books	Hindawi	REAL	FAKE	FAKE
@HindawiFoundationBooks	Hindawi	FAKE	FAKE	FAKE
@wspcsg	World Scientific	REAL	FAKE	REAL
@NaturePublishingGroup	Springer Nature	FAKE	FAKE	FAKE
@thiemepublishers	Thieme	REAL	FAKE	REAL

FAKE = fake / UNK = dubious / REAL = real