Saudi Journal of Medicine and Public Health

https://saudijmph.com/index.php/pub

https://doi.org/10.64483/202412638

Weaponized Ignorance: A Narrative Review of Digital Infodemics as a Determinant of Health Equity and National Security in the Post-Truth Era

Omad Naif Aldhafeeri [(1)] , Hamed Tarqi Alanazi [(1)] , Ahmed Asi Hassan Alshammari [(1)] , Abdullah Ali Mesfer Alharbi [(1)] , Salamah Falah Aljameeli [(1)] , Mashari Saad D Alshammari [(2)] , Faisal Asi H Alshammari [(3)] , Majed Hussain M Alanazi [(1)]

(1) Hafar Al-Batin Health Cluster King Khalid General Hospital in Hafar Al-Batin, Ministry of Health, Saudi Arabia,
(2) Hafar Al-Batin Health Cluster, Ministry of Health, Saudi Arabia,
(3) Eradah And Mintal Hospital, Hafr Al Batin, Hafar Al-Batin Health Cluster, Ministry of Health, Saudi Arabia

Abstract

Background: In the contemporary digital ecosystem, the emergence and amplification of health-related misinformation and disinformation—termed "infodemics"—has become a parallel crisis to biological pandemics. These infodemics, whether organic or deliberate, erode the foundational pillars of effective public health: trust, social cohesion, and evidence-based decision-making.

Aim: This narrative review aims to critically analyze the mechanisms and impacts of digital infodemics, framing them as a direct, non-traditional determinant of population health outcomes, health equity, and national security.

Methods: A comprehensive literature search was conducted across interdisciplinary databases (PubMed, Scopus, PsycINFO, Communication & Mass Media Complete) for peer-reviewed articles, reports, and policy documents from 2010-2024.

Results: The review identifies a triad of infodemic impacts: (1) Cognitive Sabotage, which fragments shared reality and fuels science denialism; (2) Behavioral Non-Compliance, directly reducing adherence to protective measures and vaccine uptake, disproportionately harming marginalized groups; and (3) Institutional Erosion, systematically degrading trust in health authorities and democratic institutions. These effects are often amplified by algorithmic platform architecture and, in some cases, deployed as a geopolitical strategy.

Conclusion: Digital infodemics constitute a profound threat to 21st-century health security, acting as a force multiplier for pathogens and a driver of inequity. Countering this threat requires a paradigm shift: recognizing information integrity as a public good and building multidisciplinary resilience through prebunking, strategic communication, platform accountability, and media literacy integrated into health equity frameworks.

Keywords: Infodemic, Health Disinformation, Weaponized Narratives, Health Equity, Health Security.

Introduction

The 21st century has unveiled a complex, insidious, and anthropogenic determinant of health that operates not within the confines of the human body, but within the body politic and the architecture of the collective digital mind. This threat parallels, and often exacerbates, the biological challenge of novel zoonotic spillovers (Aïmeur et al., 2023). We now confront the rapid, global propagation of health-related misinformation and disinformation—a phenomenon the World Health Organization formally classifies as an "infodemic," defined as an overabundance of information, both accurate and not, that complicates the public's ability to discern trustworthy sources and reliable guidance during a health emergency (Zarocostas, 2020). Critically, unlike a purely biological agent, this infodemic can be deliberately engineered and deployed. It is weaponized to exploit pre-existing social fractures, cognitive biases, and institutional vulnerabilities, thereby transcending public communication failure to become a potent instrument of asymmetric and hybrid conflict (Bradshaw & Howard, 2018).

Malign actors, including state and non-state entities, strategically pollute the information environment to degrade societal cohesion, erode trust in governing institutions, and sabotage coordinated crisis response (Gruzd et al., 2023). The central thesis of this narrative review is that in our contemporary post-truth era, a population's health security—its collective capacity to prevent, detect, respond to, and recover from health threats—is contingent as much upon the robustness of its **informational immune system** as upon its biological defenses. The deliberate or organic contamination of the digital public square directly corrodes the four foundational pillars of health security while simultaneously acting as an accelerant for pre-existing health inequities (Tangcharoensathien et al., 2020).

This review synthesizes interdisciplinary evidence from communication science, political psychology, public health, and security studies to

*Corresponding author e-mail: amod1438@gmail.com (Omad Naif Aldhafeeri).
Receive Date: 22 December 2024, Revise Date: 30 December 2024, Accept Date: 31 December 2024

advance the argument that digital infodemics constitute far more than a mere nuisance of false facts. They represent a **structural determinant of health outcomes**, a social pathogen that weaponizes ignorance, transforming it into a primary vector for increased disease burden, social discord, and the erosion of democratic norms, with historically marginalized and vulnerable communities disproportionately shouldering the devastating impact.

Deconstructing the Infodemic as A Spectrum of Harmful Information

An effective diagnosis and response to the infodemic phenomenon necessitates a precise and operational lexicon. The term "infodemic" encompasses a broad spectrum of harmful information, differentiated primarily by the intent of the creator or disseminator and the nature of the content (Revez & Corujo, 2024). At one end of this spectrum lies **misinformation**, which refers to false or inaccurate information that is shared without malicious intent. This often arises from genuine public fear, confusion, the complexities of rapidly evolving science, or honest misinterpretation. Examples include well-meaning individuals sharing unverified home remedies or misconstruing preliminary scientific data during the early stages of a pandemic (Wardle & Derakhshan, 2017).

In stark contrast, **disinformation** is false information that is knowingly created and disseminated with the explicit intent to deceive, manipulate, or achieve a strategic objective. This intent is what distinguishes disinformation as the core of weaponized narratives. It is frequently driven by political, ideological, or financial motives and employs sophisticated tactics such as coordinated inauthentic behavior by troll networks, the fabrication of counterfeit documents or media ("deepfakes"), and the strategic seeding of conspiracy theories to sow societal division (Freedman, 2019). A third, often overlapping category is **malinformation**. This involves the dissemination of genuine information—such as a private health record, a stolen email, or a personal detail—but shared out of its original context, in a misleading manner, or with the specific intent to harass, intimidate, or cause harm (Damasceno, 2021). An example would be doxxing a public health official to incite harassment.

The virulence and pandemic scale of this information pathology are fundamentally enabled by the underlying digital architecture of contemporary social media and search platforms. Their core business models are predicated on maximizing user engagement, attention, and time-on-site. The algorithms that curate and amplify content are, consequently, optimized to prioritize material that triggers high-arousal emotions such as outrage, fear, or moral indignation, as such content reliably generates clicks, shares, and comments (Pennycook et al., 2021). This creates a powerful, built-in incentive structure that is agnostic to truth value. False and sensational claims, which are often more novel and emotionally charged than cautious, nuanced facts, are therefore algorithmically favored, granting them superior velocity, reach, and depth of penetration within social networks. This ecosystem does not merely *allow* the spread of harmful information; it actively and systematically **amplifies** it, creating a profoundly polluted information environment that overwhelms credible voices, paralyzes public discernment, and directly impedes the rational, collective action required for an effective public health response (Van der Linden et al., 2021).

Cognitive Security and the Fragmentation of Shared Reality

The foundational impact of an infodemic is cognitive. It attacks the very possibility of a shared, evidence-based reality, a prerequisite for collective action in a health crisis. Weaponized narratives often employ strategies of "epistemic corruption," seeding doubt not just about facts, but about the institutions and processes that produce reliable knowledge (i.e., "Don't trust the experts," "Do your own research") (McIntyre, 2018). This fosters a climate of science denialism and conspiracist thinking, where complex, evolving public health guidance is reframed as evidence of elite manipulation or hidden agendas (Uscinski et al., 2020).

The false "Plandemic" narrative framed COVID-19 as a premeditated hoax for control, effectively paralyzing the cognitive ability of its adherents to engage with genuine protective measures (Kearney et al., 2020). This cognitive sabotage creates parallel informational universes, where risk perception is divorced from epidemiological reality. When a significant portion of the population inhabits a reality where the threat is minimized or fictionalized, or where the solution (e.g., vaccines) is perceived as more dangerous than the disease, the collective "herd immunity" necessary for societal response becomes impossible to achieve (Skafle et al., 2022).

Behavioral Compliance and Direct Health Impacts

Cognitive distortion directly translates into behavioral non-compliance, with measurable negative health outcomes. Infodemics have been empirically linked to reduced adherence to non-pharmaceutical interventions (NPIs) like masking and social distancing, and to decreased vaccine uptake (Karami et al., 2021). Studies during the COVID-19 pandemic consistently found that higher exposure to misinformation was a strong predictor of vaccine hesitancy and refusal (Loomba et al., 2021; Roozenbeek et al., 2020). This is not a passive correlation but often a result of targeted campaigns. Anti-vaccine networks, for instance, have evolved into sophisticated, globally connected "misinformation ecosystems," using emotionally resonant personal narratives, appropriated scientific imagery, and targeted advertising to dissuade vaccination (Broniatowski et al., 2018). The consequence is the prolongation of outbreaks, increased hospitalization

and mortality rates, and the failure to reach critical vaccination thresholds. The behavioral impact thus transforms the infodemic from an information problem into a direct driver of morbidity and mortality, effectively making disinformation a pathogenic agent (Béchard et al., 2024).

Institutional Trust and the Crippling of Response

Effective public health relies on a compact of trust between citizens and institutions—government agencies, healthcare systems, and scientific bodies. Infodemics are meticulously engineered to sever this trust. By framing health authorities as corrupt, incompetent, or tyrannical, weaponized narratives destroy the social license needed to implement potentially disruptive but necessary measures (Kuatewo et al., 2024). This erosion is asymmetric; rebuilding trust is slow and arduous, while destroying it can be achieved rapidly through viral lies. The MMR vaccine-autism fraud, despite being thoroughly debunked, continues to damage public confidence in immunization programs decades later (DeStefano & Shimabukuro, 2019). During COVID-19, coordinated disinformation campaigns portrayed public health leaders as participants in a "deep state" plot, directly impeding the rollout of guidance and vaccines (Evanega et al., 2020). This institutional erosion paralyzes the command-and-coordination functions at the heart of health security, leaving societies unable to mount a unified, timely, and effective defense against a biological threat (Evanega et al., 2023).

Infodemics as Amplifiers of Structural Vulnerability

The harms of infodemics are not distributed equally; they systematically compound existing health inequities, acting as a threat multiplier for marginalized populations. Vulnerable groups—including racial and ethnic minorities, low-income communities, and those with lower health or digital literacy—often face a "double burden": higher biological risk from the pathogen and higher exposure to targeted misinformation (Ferrara et al., 2024). Algorithmic profiling can allow disinformation actors to micro-target these communities with tailored narratives that exploit historical traumas and legitimate grievances with the medical system (the Tuskegee syphilis study) to foster distrust in current interventions (Murdan et al., 2023). Furthermore, limited access to credible, culturally competent health information creates a vacuum readily filled by misinformation. The result is a widening of disparities in protective behaviors, infection rates, and vaccination coverage, transforming the infodemic into a powerful engine of social injustice. It weaponizes pre-existing inequities, ensuring that the most vulnerable bear the highest cost of the information disorder (Dickson et al., 2023).

Infodemics as Tools of Hybrid Warfare

Beyond public health, infodemics represent a clear and present danger to national and international security. The weaponization of information is now a standard tool in hybrid warfare, used by state and non-state actors to weaken adversarial societies from within (Carley, 2020). By deliberately sowing confusion, fear, and division around health crises, malign actors can degrade social cohesion, overwhelm crisis response mechanisms, and destabilize political systems. The goal is to reduce a state's resilience and operational capacity, making it more vulnerable to a range of threats (Shin et al., 2024). The NATO StratCom Centre of Excellence has explicitly identified health-related disinformation as a security threat, noting its use to undermine alliance solidarity and weaken democratic governance (Reding & Wells, 2022). In this light, an infodemic is not a byproduct of a pandemic but can be a primary attack vector—a non-kinetic weapon that achieves strategic objectives by turning a society's own information ecosystem against it, compromising its ability to protect the health and well-being of its citizens (Table 1).

Table 1: The Typology and Impact of Weaponized Health Narratives

Narrative Archetype	Primary Objective	Common Tactics	Direct Health Security Impact	Equity Dimension
The "Corrupt Elite" / "Plandemic"	Erode trust in institutions & science.	Fabricated documents; impersonation of experts; claims of hidden financial/power motives.	Non-compliance with all NPIs and medical countermeasures; paralysis of public health response.	Exploits existing political and class-based distrust.
The "Dangerous Intervention"	Sabotage specific medical tools (e.g., vaccines, therapeutics).	Misrepresented data; cherry-picked anecdotes (e.g., VAERS reports); pseudo-scientific jargon.	Reduced vaccine uptake; treatment refusal; prolongation of outbreaks.	Often targets parents & communities with historical medical trauma.
The "Minimized Threat"	Reduce risk perception &	False comparisons (e.g., "just the flu"); downplaying	Increased transmission via risky	Disproportionately harms high-risk

	encourage inaction.	case/death counts; promoting natural immunity myths.	behavior; delayed care-seeking.	groups who adopt this narrative.
The "Divisive Scapegoat"	Foster social fragmentation & blame.	Blaming outbreak on specific ethnic/religious groups; promoting "us vs. them" in resource access.	Undermines social cohesion needed for collective action; incites violence.	Directly targets and stigmatizes minority populations, worsening outcomes.
The "Miracle Cure"	Promote alternative (often profitable) products; discredit mainstream medicine.	Celebrity endorsements; fake patient testimonials; attacks on regulatory agencies as "suppressive."	Poisonings (e.g., ivermectin, bleach); abandonment of effective care; drug shortages.	Preys on the desperate and those with limited healthcare access.

Countermeasures in Building Resilience in the Digital Immune System

Combating weaponized infodemics demands a paradigm shift from reactive correction to proactive, systemic immunization of the information ecosystem. Analogous to building biological herd immunity, this endeavor requires a multi-layered defense strategy that addresses vulnerability at societal, technological, and individual levels. While reactive fact-checking remains a necessary component, it is often outmatched by the scale, emotional resonance, and sophisticated delivery of coordinated disinformation (Lewandowsky et al., 2012). Therefore, effective countermeasures must operate upstream to prevent infection, midstream to limit transmission, and downstream to treat exposure.

A cornerstone of this proactive approach is **prebunking, grounded in inoculation theory**. This method involves preemptively exposing individuals to weakened forms of misleading arguments and manipulative rhetorical tactics (e.g., emotional language, false dichotomies, impersonated experts), thereby building cognitive antibodies before encountering real-world disinformation (Compton et al., 2021; van der Linden et al., 2017). Research indicates that this "psychological vaccination" can significantly reduce subsequent susceptibility to misinformation by teaching people to recognize the hallmarks of manipulation rather than debunking endless specific falsehoods. A second critical layer involves the strategic deployment of **trusted messenger engagement**. In contexts of eroded institutional trust, information credibility is conferred not by the source's authority but by its perceived affinity and shared identity. Partnering with credible, culturally aligned community figures—such as local healthcare providers, faith leaders, or respected grassroots organizers—can bypass skepticism toward national institutions and deliver accurate health guidance through pre-existing channels of trust (Abad et al., 2024; Goldberg et al., 2021).

The technological architecture that facilitates infodemics must itself be a target of intervention, necessitating **platform accountability and algorithmic transparency**. The dominant business models of social media platforms, which optimize for user engagement, inadvertently favor content that evokes strong emotions like outrage and fear, thereby amplifying misinformation (Vosoughi et al., 2018). Regulatory frameworks and sustained public pressure are required to compel platforms to redesign recommendation algorithms to prioritize authenticity and authoritative sourcing, audit them for discriminatory impacts, and enforce consistent, transparent policies against harmful health disinformation (Donovan, 2020; Gillespie, 2018). Finally, building population-level resilience requires **integrated media and health literacy** as a fundamental educational component. This extends beyond traditional health education to include critical digital literacy: teaching individuals to recognize inauthentic accounts, verify sources using lateral reading techniques, understand scientific processes like peer review, and identify common logical fallacies (Guess & Munger, 2023; Breakstone et al., 2021). Embedding these skills in school curricula and adult public health campaigns cultivates a more discerning public, less vulnerable to manipulation.

Implementing these diverse strategies requires a coherent, tiered framework that aligns actors, objectives, and tools across different levels of the information ecosystem. As summarized in **Table 2**, a comprehensive defense integrates upstream efforts to build societal resilience, midstream interventions to sanitize the digital environment, downstream public health actions for rapid response, and strategic legal-normative measures to impose costs on malicious actors.

Table 2: A Layered Defense Framework Against Weaponized Health Infodemics

Layer of Defense	Objective	Key Strategies & Actors	Challenges

Upstream: Societal Resilience	Build population-wide cognitive immunity.	Integrate media literacy into national education curricula; fund public science communication.	Long-term investment, political will, and avoiding partisan framing of literacy.
Midstream: Platform & Ecosystem	Reduce the velocity and reach of falsehoods.	Algorithmic transparency & reform; consistent labeling/removal of harmful disinformation; support for credible health creators.	Balancing free expression, corporate profit motives, and global platform governance.
Downstream: Public Health Response	Ensure accurate information reaches all communities effectively.	Proactive prebunking campaigns; deployment of trusted community messengers; rapid rumor surveillance and rebuttal.	Requires real-time capacity; building trust networks is slow and resource-intensive.
Strategic: Legal & Normative	Impose costs on malicious actors and state sponsors.	Designating health disinformation as a national security threat, international cooperation on attribution and sanctions, and updating broadcast/licensing regulations.	Geopolitical tensions, defining legal thresholds, and risks to civil liberties.

Conclusion

The evidence is unequivocal: digital infodemics, particularly when weaponized, are a direct and potent determinant of 21st-century health outcomes, equity, and security. They represent a man-made vulnerability that can turn a manageable outbreak into a catastrophic crisis. Addressing this threat requires a paradigm shift in public health and governance. We must move beyond viewing misinformation as mere "noise" and recognize information integrity as a foundational public good, as critical to societal health as clean water or air. Defending it demands breaking down silos between public health, national security, technology governance, and education. The battle against the next pathogen will be fought not only in labs and clinics but in the feeds, forums, and shared narratives of the digital public square. Building resilient, equitable, and informed societies is therefore the ultimate preparedness strategy—one that strengthens our defenses against both biological and ideological contagions.

References

1. Abad, N., Bonner, K. E., Kolis, J., Brookmeyer, K. A., Voegeli, C., Lee, J. T., ... & Cohn, A. (2024). Strengthening COVID-19 vaccine confidence & demand during the US COVID-19 emergency response. *Vaccine*, *42*, 125604. https://doi.org/10.1016/j.vaccine.2024.01.029
2. Aïmeur, E., Amri, S., & Brassard, G. (2023). Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*, *13*(1), 30. https://doi.org/10.1007/s13278-023-01028-5
3. Béchard, B., Gramaccia, J. A., Gagnon, D., Laouan-Sidi, E. A., Dubé, È., Ouimet, M., ... & Tremblay, S. (2024). The resilience of attitude toward vaccination: Web-based randomized controlled trial on the processing of misinformation. *JMIR Formative Research*, *8*, e52871. https://doi.org/10.2196/52871
4. Bradshaw, S., & Howard, P. N. (2018). The global organization of social media disinformation campaigns. *Journal of International Affairs*, *71*(1.5), 23-32. https://www.jstor.org/stable/26508115
5. Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., ... & Dredze, M. (2018). Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate. *American journal of public health*, *108*(10), 1378-1384. https://doi.org/10.2105/AJPH.2018.304567
6. Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and mathematical organization theory*, *26*(4), 365-381. https://doi.org/10.1007/s10588-020-09322-9
7. Compton, J., Van Der Linden, S., Cook, J., & Basol, M. (2021). Inoculation theory in the post-truth era: Extant findings and new frontiers for contested science, misinformation, and conspiracy theories. *Social and Personality Psychology Compass*, *15*(6), e12602. https://doi.org/10.1111/spc3.12602
8. Damasceno, C. S. (2021). Multiliteracies for combating information disorder and fostering civic dialogue. *Social Media+ Society*, *7*(1), 2056305120984444. https://doi.org/10.1177/2056305120984444
9. DeStefano, F., & Shimabukuro, T. T. (2019). The MMR vaccine and autism. *Annual review of virology*, *6*(1), 585-600.

https://doi.org/10.1146/annurev-virology-092818-015515
10. Dickson, K., Aboltins, C., Pelly, J., & Jessup, R. L. (2023). Effective communication of COVID-19 vaccine information to recently-arrived culturally and linguistically diverse communities from the perspective of community engagement and partnership organisations: a qualitative study. *BMC Health Services Research*, *23*(1), 877. https://doi.org/10.1186/s12913-023-09836-3
11. Donovan, J. (2020). Concrete recommendations for cutting through misinformation during the COVID-19 pandemic. *American journal of public health*, *110*(S3), S286-S287. https://doi.org/10.2105/AJPH.2020.305922
12. Evanega, S., Lynas, M., Adams, J., Smolenyak, K., & Insights, C. G. (2020). Coronavirus misinformation: quantifying sources and themes in the COVID-19 'infodemic'. *JMIR Preprints*, *19*(10), 2020.
13. Evanega, S., Lynas, M., Adams, J., & Smolenyak, K. (2023). *Coronavirus misinformation: Quantifying sources and themes in the COVID-19 'infodemic.'[Internet]*. *2020*.
14. Ferrara, M., Langiano, E., Esposito, M., Lo Moro, G., Lombardi, R., Vuolanto, P., & De Vito, E. (2024). Key factors in complex public health interventions to address vaccine hesitancy using a multidisciplinary approach: the VAX-TRUST project. *Health Education Research*, *39*(6), 487-494. https://doi.org/10.1093/her/cyae027
15. Freedman, L. (2019). *Ukraine and the Art of Strategy*. Oxford University Press.
16. Gruzd, A., Tangcharoensathien, V., Calleja, N., Nguyen, T., Purnat, T., D'Agostino, M., ... & Briand, S. (2023). Framework for Managing the COVID-19 Infodemic: Methods and Results of an Online, Crowdsourced WHO Technical Consultation. https://doi.org/10.32920/21992087
17. Guess, A. M., & Munger, K. (2023). Digital literacy and online political behavior. *Political science research and methods*, *11*(1), 110-128. doi:10.1017/psrm.2022.17
18. Karami, A., Lundy, M., Webb, F., Turner-McGrievy, G., McKeever, B. W., & McKeever, R. (2021). Identifying and analyzing health-related themes in disinformation shared by conservative and liberal Russian trolls on twitter. *International journal of environmental research and public health*, *18*(4), 2159. https://doi.org/10.3390/ijerph18042159
19. Kearney, M. D., Chiang, S. C., & Massey, P. M. (2020). The Twitter origins and evolution of the COVID-19 "plandemic" conspiracy theory. *Harvard Kennedy School Misinformation Review*, *1*(3). https://doi.org/10.37016/mr-2020-42
20. Kuatewo, M., Ebelin, W., Doegah, P. T., Kpodo, L., Kpordorlor, A. G., Lissah, S., ... & Ansah, E. (2024). "People will not even bring out their children to be immunised, because of the corona vaccine": fake news, misinformation, vaccine hesitancy and the role of community engagement in COVID-19 vaccine acceptance in Southern Ghana. *medRxiv*, 2024-12. https://doi.org/10.1101/2024.12.22.24319502
21. Loomba, S., De Figueiredo, A., Piatek, S. J., De Graaf, K., & Larson, H. J. (2021). Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA. *Nature human behaviour*, *5*(3), 337-348. https://doi.org/10.1038/s41562-021-01056-1
22. McIntyre, L. (2018). *Post-truth*. MIt Press.
23. Murdan, S., Ali, N., Darlow, J., Christopher, E., Tolani, F., & Ashiru-Oredope, D. (2023). Enhancing the training of community engagement officers to address vaccine hesitancy: a university and local authority collaboration. *Perspectives in Public Health*, *143*(4), 190-192. https://doi.org/10.1177/17579139221145616
24. Pennycook, G., Binnendyk, J., Newton, C., & Rand, D. G. (2021). A practical guide to doing behavioral research on fake news and misinformation. *Collabra: Psychology*, *7*(1), 25293. https://doi.org/10.1525/collabra.25293
25. Reding, D. F., & Wells, B. (2022). Cognitive warfare: NATO, COVID-19 and the impact of emerging and disruptive technologies. In *COVID-19 Disinformation: A Multi-National, Whole of Society Perspective* (pp. 25-45). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-94825-2_2
26. Revez, J., & Corujo, L. (2024). Scientists' behaviour towards information disorder: A systematic review. *Journal of Information Science*, 01655515241244460. https://doi.org/10.1177/01655515241244460
27. Roozenbeek, J., Schneider, C. R., Dryhurst, S., Kerr, J., Freeman, A. L., Recchia, G., ... & Van Der Linden, S. (2020). Susceptibility to misinformation about COVID-19 around the world. *Royal Society open science*, *7*(10), 201199. https://doi.org/10.1098/rsos.201199
28. Shin, J., Dobson, G. B., Carley, L. R., & Carley, K. M. (2024, December). Design,

Modeling and Simulation of Cybercriminal Personality-Based Cyberattack Campaigns. In *2024 Winter Simulation Conference (WSC)* (pp. 2058-2069). IEEE. https://doi.org/10.1109/WSC63780.2024.10838743

29. Skafle, I., Nordahl-Hansen, A., Quintana, D. S., Wynn, R., & Gabarron, E. (2022). Misinformation about COVID-19 vaccines on social media: rapid review. *Journal of medical Internet research*, *24*(8), e37367. https://doi.org/10.2196/37367
30. Tangcharoensathien, V., Calleja, N., Nguyen, T., Purnat, T., D'Agostino, M., Garcia-Saiso, S., ... & Briand, S. (2020). Framework for managing the COVID-19 infodemic: methods and results of an online, crowdsourced WHO technical consultation. *Journal of medical Internet research*, *22*(6), e19659. https://doi.org/10.2196/19659
31. Uscinski, J. E., Enders, A. M., Klofstad, C., Seelig, M., Funchion, J., Everett, C., ... & Murthi, M. (2020). Why do people believe COVID-19 conspiracy theories?. *Harvard Kennedy School Misinformation Review*, *1*(3). https://doi.org/10.37016/mr-2020-015
32. Van der Linden, S., Roozenbeek, J., Maertens, R., Basol, M., Kácha, O., Rathje, S., & Traberg, C. S. (2021). How can psychological science help counter the spread of fake news?. *The Spanish journal of psychology*, *24*, e25. doi:10.1017/SJP.2021.23
33. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *science*, *359*(6380), 1146-1151. https://doi.org/10.1126/science.aap9559
34. Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking* (Vol. 27, pp. 1-107). Strasbourg: Council of Europe.
35. Zarocostas, J. (2020). How to fight an infodemic. *The lancet*, *395*(10225), 676. https://doi.org/10.1016/S0140-6736(20)30461-X.