ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2024 (35)

DISINFORMATION SUPPORTED BY ARTIFICIAL INTELLIGENCE FROM DYNAMIC RESEARCH TO HOLISTIC SOLUTIONS

Krunoslav ANTOLIŠ
University of Applied Sciences in Criminal Investigation and Public Security
Police academy "First Croatian Police Officer"
Ministry of Internal Affairs
Republic of Croatia, Av Gojka Šuška 1
E-mail kantolis@fkz.hr
ORCID ID:0009-0002-6203-7522

DOI: 10.13165/PSPO-24-35-02

Abstract. *This paper investigates the intricate interplay between artificial intelligence (AI) and the proliferation of disinformation, presenting a strategic framework to mitigate its impact in the digital era. The study encompasses diverse domains, contributing to a comprehensive grasp of AI-driven disinformation. It delves into the dynamics of disinformation, scrutinizing the mechanisms of creation and dissemination, with a particular focus on the role played by AI. The methods employed involve analyzing AI involvement, enhancing algorithms for real-time recognition and analysis of disinformation, and exploring social dynamics and human behavior.*
The research unveils the tactics employed by malicious entities, such as fabricating misleading naratives and manipulating information. Agile AI algorithms have been devised for assessing credibility, tracking geolocation, and implementing ethical privacy protection measures. The implications encompass identifying social structures and cognitive vulnerabilities, leading to the development of targeted interventions.
An AI-centric detection approach revolves around refining algorithms for real-time identification of disinformation, emphasizing credibility assessment, geolocation tracking, and privacy protection measures. The aim is to fortify systems with the capability to swiftly detect disinformation.
The assessment of social and psychological factors delves into the influence of social structures, group dynamics, and cognitive biases on the propagation of disinformation. Educational programs are being formulated to enhance awareness and critical thinking, with strategies tailored to address specific vulnerabilities.
Cross-sectoral collaboration underscores the importance of information exchange between sectors, pooling expert knowledge, and establishing communication channels. Collaborative efforts with technology companies, educational institutions, and others enable a comprehensive approach to combat disinformation.
Balancing regulation and fundamental rights grapples with the challenges of preserving freedom of speech and privacy. Defining the equilibrium of legal frameworks, considering the global context and the dynamic nature of technology, is essential. Transparency and ethical considerations play a pivotal role in regulatory measures.
Public awareness and education initiatives aim to reduce susceptibility to disinformation. Awareness campaigns inform about the existence of disinformation, while educational programs foster media literacy and critical thinking skills. Evaluation involves measuring the level of awareness and assessing changes in behavior.
In summary, this research offers insights for a holistic approach to address the challenges posed by AI-driven disinformation. The proposed framework encourages interdisciplinary collaboration, underscores ethical considerations in regulation, and advocates for education and awareness.

Keywords: *disinformation, social, awareness, strategies, media*

Introduction

This paper thoroughly investigates the intricate corelation between artificial intelligence (AI) and the proliferation of disinformation, laying the groundwork for constructing a strategic framework to effectively mitigate the impact of disinformation in the digital age. The research encompasses various yet interconnected domains, collectively contributing to a comprehensive comprehension and response to the challenges presented by AI-enabled disinformation.

Purpose. The aim is to scrutinize the mechanisms and tactics involved in the creation and dissemination of disinformation, with a specific emphasis on AI. Some fake news are so similar to the real ones that it is difficult for human to identify them. Therefore, automated fake news detection tools like machine learning and deep learning models have become an essential requirement (Jiang et al. 2021). The objective is to develop and enhance artificial intelligence algorithms tailored for real-time identification and analysis of disinformation.

Methods. Examine the multifaceted processes behind disinformation creation, including an in-depth exploration of AI involvement for enhanced understanding. Upgrade algorithms for real-time credibility assessment, integrate geolocation tracking, and implement privacy protection measures. Conduct thorough research on human behavior and the social dynamics fueling disinformation, highlighting group dynamics, cognitive biases, vulnerabilities, and emotional triggers. Facilitate information exchange, leverage sector-specific expertise, and establish real-time communication channels for coordinated responses. Evaluate the impact of regulatory measures on free speech, privacy, and ethical considerations. Employ surveys, focus groups, and analytics to measure awareness, behavioral change, and the long-term sustainability of knowledge. As (Demartini et al. , 2020) argued, human-in-the-loop AI (HAI) systems combine the best of both worlds, with humans filtering what will be implemented in practice by a machine that performs tasks based on databases and machine learning algorithms.

Findings. Uncover the intricate strategies employed by malicious entities, addressing the creation of deceptive stories, manipulation of information, and exploitation of vulnerabilities in communication channels. The development process includes agile AI algorithms for credibility assessment, geolocation tracking to understand dissemination patterns, and ethical privacy safeguards.

Implications. Identify social structures and cognitive vulnerabilities contributing to disinformation, leading to the development of targeted interventions. Emphasize collaboration in leveraging unique datasets, combining legal perspectives, geopolitical insights, and technological expertise. Address the delicate balance between countering disinformation and protecting individual rights, emphasizing transparent and democratic regulatory processes. Evaluate the effectiveness of initiatives in fostering media literacy, critical thinking, and responsible information sharing. The insights aim to enhance understanding of the evolving disinformation landscape, ultimately contributing to the development of effective mitigation strategies. The goal is to contribute to advanced tools combating the spread of false information in the digital domain. Strategies include educational programs, media literacy initiatives, and promoting critical thinking to address the root causes of disinformation consumption. Advocate for partnerships to develop comprehensive, interdisciplinary approaches to combat multiple disinformation campaigns. Call for international cooperation, the creation of ethical policies, and iterative adjustments to regulatory frameworks. Advocate for ongoing evaluation, collaborative efforts, and a nuanced approach to shaping an informed and resilient digital society.

This comprehensive research offers valuable insights for developing a holistic strategy to address the challenges arising from the interplay of AI and disinformation. The proposed framework encourages interdisciplinary collaboration, underscores ethical considerations in regulation, and aims to empower the public through education and awareness. Study discusses a long-term strategy to develop models for predicting fake news before it spreads and to research the effectiveness of personalized intervention mechanisms (Fátima C.(2023). The combination of AI and blockchain technologies, such as in the practice of fact-checking,

encompasses the three stages of fact-checking: identification, verification, and distribution (Graves, 2018); (Nakov et al., 2021), (Westlund et al., 2022) pointed out that the identification stage gathers the highest concentration of technologies.

Understanding the Dynamics of Disinformation

To comprehend the dynamics of disinformation, it is essential to delve into the mechanisms and tactics employed in the creation and dissemination of misleading information, including the role of artificial intelligence (AI) in these processes. Grasping the dynamics of disinformation necessitates an exploration of the methods and strategies utilized in its origination and circulation. This entails a thorough examination of how artificial intelligence (AI) contributes to these disinformation processes.

In this facet of investigation, the emphasis should be on revealing the intricate methods by which disinformation is generated and propagated. It is crucial to scrutinize the mechanisms utilized by malicious actors, such as fabricating false naratives, manipulating information, and exploiting vulnerabilities in communication channels. The inquiry should center on evaluating the involvement of artificial intelligence, understanding how advanced technologies enhance the sophistication and scale of disinformation campaigns. By scrutinizing these dynamics, the research aims to enhance our comprehension of the evolving disinformation landscape, ultimately contributing to the formulation of effective strategies and countermeasures to mitigate its impact. The objectives were to uncover the organization and dynamics of this "system" and provide insights into the content, strategies, and motivations driving the circulation of information.

The initial goals included:

Applying methods for examining online misinformation, as outlined in (Maddock et al., 2015), to identify multi-dimensional indicators of disinformation propagation on the internet.

Revealing the structure and tactics employed by the alternative media ecosystem that facilitates disinformation, such as mapping social media communities and the network of domains involved in creating, hosting, remixing, and sharing this content. This involves exposing connections between social media accounts, communities, web domains, authors, and more.

Investigating common disinformation trajectories, analyzing how information moves across different structures and understanding how these structures influence those trajectories.

Distinguishing between emergent and orchestrated properties of the ecosystem, addressing whether the dissemination of information is primarily driven by financial opportunists creating content for ad revenue or by political actors strategically spreading specific stories by seeding content on particular sites. The insights gleaned from this research will play a pivotal role in constructing a more resilient and informed digital society.

Developing an AI-Powered Detection Method

AI-powered threat detection and prevention technologies have become increasingly significant in cybersecurity. These technologies enable organizations to analyze vast amounts of data in real time, detect potential threats, and respond swiftly. Despite the challenges and ethical considerations, AI holds great promise for the future of cybersecurity, with advancements in threat detection and response systems expected to redefine the industry. By

harnessing the power of AI and fostering collaboration, organizations can enhance their cybersecurity capabilities and stay ahead of evolving threats. The development of an AI-based detection method involves the creation and enhancement of AI algorithms and tools tailored specifically for the identification and analysis of disinformation. The primary emphasis lies in augmenting capabilities that facilitate real-time credibility assessment, the incorporation of geolocation tracking, and the implementation of measures to safeguard privacy.

In the domain of real-time credibility assessment, the primary focus is on constructing artificial intelligence algorithms capable of swiftly and accurately evaluating the credibility of information as it surfaces. This encompasses the evaluation of the reliability and credibility of sources, content, and contextual information in real-time.

Regarding geolocation tracking, the crucial integration of this feature into artificial intelligence systems enables the analysis of the geographical origin and dissemination patterns of disinformation. This capability aids in comprehending the scope of disinformation campaigns and tailoring responses based on geographic trends.

As artificial intelligence tools become involved in the scrutiny of potentially sensitive information, ensuring privacy protection becomes paramount. The development process incorporates measures to uphold individuals' right to privacy while effectively identifying and countering disinformation.

Continuous refinement of AI algorithms is imperative to adapt to the ever-evolving nature of disinformation tactics. This involves the integration of machine learning techniques, monitoring emerging disinformation strategies, and adjusting algorithms accordingly.

The AI-centric approach transcends simple content analysis, encompassing a multifaceted examination that considers context, intent, and dissemination patterns. This holistic analysis significantly enhances the accuracy of disinformation detection.

Collaboration with experts in fields such as cybersecurity, data science, and privacy law is an integral aspect of the development process. Bringing together diverse perspectives ensures a comprehensive and effective AI-based detection approach.

The overarching objective of developing this AI-based detection approach is to empower systems with the capability to swiftly and accurately identify disinformation in real-time. By concentrating on credibility assessments, geolocation tracking, and privacy protection measures, the research aims to contribute to the creation of advanced tools that can play a pivotal role in countering the spread of false information in the digital realm.

Evaluating Social and Psychological Factors

The assessment of social and psychological factors entails a thorough examination of the elements within human behavior and social dynamics that play a role in disseminating disinformation. The objective is to comprehend these factors and subsequently devise strategies to counteract their influence. Key aspects of this evaluation include:

- Investigating how social structures, group dynamics, and interpersonal relationships contribute to the dissemination of disinformation. This involves understanding how disinformation can be amplified within echo chambers, social networks, and online communities.
- Analyzing cognitive biases, psychological vulnerabilities, and emotional triggers that render individuals susceptible to believing and sharing disinformation. Grasping these

factors is crucial for designing interventions that address the underlying causes of disinformation consumption.

- Developing educational programs with the aim of increasing awareness about common cognitive biases and logical erors. By equipping individuals with tools for critical information evaluation, these initiatives seek to empower the public to differentiate between true and false content.
- Initiating efforts to enhance media literacy skills among the general population. This includes educating individuals on how to navigate and critically evaluate information from various sources, encompassing online platforms, traditional media, and social media.
- Encouraging the development of critical thinking skills that enable individuals to question information, verify sources, and contextually analyze content. Critical thinking serves as a fundamental defense against the inadvertent or deliberate spread of disinformation.
- Tailoring strategies to address specific social and psychological vulnerabilities identified through research. This may involve targeted interventions for certain demographic groups or online communities particularly susceptible to disinformation.
- Collaborating with experts in psychology, sociology, and related fields to gain a deeper insight into human behavior. This interdisciplinary approach provides a more nuanced understanding of the social and psychological factors in play.
- Recognizing that countering disinformation requires not only short-term interventions but also long-term behavior change. This includes establishing sustainable educational efforts to foster a culture of critical thinking and media literacy.

There are basically three types of interventions that can be undertaken in the search for solutions, namely automation, education and regulation, which we can propose as a set of holistic measures to detect, and potentially control, predict and prevent the further spread of misinformation. Automated solutions help (but do not replace) human judgments about whether news is true and credible. Information literacy efforts require further in-depth understanding of the phenomenon and interdisciplinary collaboration beyond traditional library and information science, including media studies, journalism, interpersonal psychology, and communication perspectives. Through systematic research and understanding of the social and psychological factors contributing to disinformation spread, the aim is to promote the development of effective strategies. Rooted in education, media literacy, and critical thinking, these strategies seek to cultivate a more resilient and discerning public capable of navigating the complex information landscape of the digital age.

Collaboration Across Sectors

The collaborative approach across sectors underscores the significance of joint endeavors involving entities such as law enforcement, intelligence agencies, technology companies, and educational institutions to effectively combat disinformation. The key aspects of this collaborative strategy include:

- Essential facilitation of information exchange between diverse sectors. Law enforcement, intelligence agencies, and technology companies possess distinct datasets and insights that, when shared appropriately, enhance the collective ability to identify and counter disinformation campaigns.

- Integration of expertise from various sectors ensures a more comprehensive understanding of the multifaceted nature of disinformation. Law enforcement contributes legal perspectives, intelligence agencies offer insights into geopolitical contexts, and technology companies provide technical expertise.
- Establishment of real-time communication channels for information exchange enables swift responses to emerging threats of disinformation. Collaborative efforts enable a coordinated and effective response to mitigate the impact of false information before it spreads.
- Cooperation with law enforcement authorities aids in developing and implementing legal frameworks aimed at preventing and penalizing disinformation activities. This collaboration ensures that the response to disinformation is not solely technological but also legal and regulatory.
- Collaboration with technology companies is crucial for leveraging advanced tools and algorithms. This partnership can lead to the creation of innovative technologies for large-scale detection and countering of disinformation.
- Involvement of educational institutions is vital for implementing long-term solutions. These institutions can contribute to the development of educational programs that promote media literacy, critical thinking, and digital citizenship skills among the public.
- Encouragement of partnerships between the public and private sectors ensures a holistic approach. Private companies often possess insights into online behavior, algorithms, and user patterns, making their cooperation essential in the fight against disinformation.
- Collaboration helps manage ethical considerations associated with combating disinformation. Bringing together stakeholders from different sectors allows for a balanced approach that takes into account legal, privacy, and human rights implications.
- Acknowledging that disinformation is a global challenge, international cooperation is imperative. Coordination between countries and international organizations enhances the effectiveness of efforts to combat disinformation across borders.
- Joint efforts can support research and development initiatives to stay ahead of evolving disinformation tactics. This includes continuous innovation in technologies and strategies to counter new and sophisticated methods of disinformation.

(Kate Starbird et all, 2019) argue that strategic information operations (e.g. disinformation, political propaganda, and other forms of online manipulation) are a critical concern for CSCW researchers, and that the CSCW community can provide vital insight into understanding how these operations function-by examining them as collaborative "work" within online crowds. Through a sociotechnical lens, we contribute a more nuanced understanding of these operations (beyond "bots" and "trolls") and highlight a persistent challenge for researchers, platform designers, and policy makers-distinguishing between orchestrated, explicitly coordinated, information operations and the emergent, organic behaviors of an online crowd.

In summary, cross-sector collaboration is a strategic necessity in the battle against disinformation. By fostering collaboration among law enforcement, intelligence agencies, technology companies, and educational institutions, a more robust and holistic approach can be developed to address the multifaceted challenges posed by disinformation campaigns.

Balancing Regulation and Fundamental Rights

Navigating the delicate balance between regulation and fundamental rights entails a nuanced examination of challenges and ethical considerations associated with regulating disinformation while upholding core principles such as freedom of speech and privacy. The key facets of this intricate issue include:

- Balancing the counteraction of disinformation with the preservation of freedom of speech poses a significant challenge. Regulatory measures must be meticulously crafted to prevent encroachment on individuals' rights to express opinions and ideas, even if those opinions are unpopular or controversial.
- Privacy considerations must be factored into regulatory responses to disinformation. Measures like content moderation and data collection for monitoring disinformation raise concerns about safeguarding individuals' personal data. Striking a balance involves reconciling the need for information security with the right to privacy.
- Crafting regulatory frameworks effective in combating disinformation without infringing on fundamental rights requires finesse. Achieving balance necessitates defining clear guidelines, ensuring accountability, and incorporating transparent and democratic processes in regulatory formulation.
- Recognizing the global scope of disinformation, regulatory efforts should consider international standards. Collaborative endeavors between countries and international organizations can establish common principles and guidelines to address disinformation while respecting fundamental rights.
- Regulating disinformation requires careful consideration of how measures may impact public discourse. Excessively restrictive regulations could inadvertently stifle legitimate debate and dissent. Striking the right balance involves addressing disinformation without suppressing diverse opinions.
- The dynamic nature of technology adds complexity to regulation. The rapid evolution of online platforms and communication channels demands flexible and adaptive regulatory approaches that effectively combat disinformation without impeding technological innovation.
- Balanced regulation encompasses not only legal measures but also educational initiatives. Promoting media literacy and critical thinking empowers individuals to distinguish reliable information from falsehoods, reducing the reliance on overly restrictive regulations.
- Ethical considerations take center stage in disinformation regulation. Policymakers must navigate a fine line between protecting society from harmful disinformation and upholding ethical standards that respect the rights and dignity of individuals.
- Ensuring transparency in the decision-making processes of regulatory authorities is crucial. Transparent procedures build trust and ensure that regulatory actions align with democratic principles, being accountable, fair, and consistent.
- Acknowledging the evolving nature of the disinformation challenge, regulatory frameworks should undergo periodic assessment and adjustment. This iterative process allows for continuous improvement and adaptation to emerging threats.

The platforms should stick to their intermediary role and empower users to develop the information landscape through their choices. In this sense, platforms should ensure ideological

neutrality of their content moderation and refrain from discriminating, while respecting human rights.

In conclusion, exploring the challenges and ethical considerations in balancing regulations and fundamental rights demands a thoughtful and multidimensional approach. Striking the right balance entails crafting regulations that effectively combat disinformation while safeguarding the principles of free speech and privacy fundamental to democratic societies.

Public Awareness and Education

Public awareness and education focus on evaluating the effectiveness of campaigns and programs designed to inform and educate the public, aiming to reduce susceptibility to disinformation and cultivate a more informed digital society.

Fake news is present not only in alternative sources but also within mainstream media. Therefore, it is crucial for key figures in mainstream media, including journalists and editors, to enhance their abilities in identifying fake news. This is particularly important when utilizing online sources for news production to avoid the dissemination of misinformation. These media professionals should actively participate in Media and Information Literacy (MIL) education, informing their audiences about the phenomenon and assisting them in acquiring the skills necessary to discern the authenticity of news and information.

To address this, MIL should be integrated into mainstream educational curricula at all levels and regularly updated to meet current demands. It is essential for news consumers to seize opportunities to become media and information literate. Additionally, MIL programs should consider effective methods for training individuals without formal education. Identifying knowledgeable gatekeepers within communities can be one approach, as they can serve as reliable sources for authenticating the credibility and accuracy of news and information.

The study underscores the significance of fact-checking as a crucial skill for media and information consumers in combating misinformation, disinformation, and malinformation. Proficiency in techniques such as reverse image searches, assessing technical flaws in news stories, utilizing fact-checking websites, and identifying clone news websites is imperative.

Lastly, the research recommends further exploration into media and information literacy within both digital and traditional media realms. This should include investigating related issues like cyberbullying, privacy, and security in the digital sphere. Understanding cybersecurity, experiences with cyber theft and cyberbullying, and individuals' strategies for staying safe online are particularly relevant given the central role of digital technologies in contemporary lifestyles.

Here are the key components for comprehending and assessing the impact of these initiatives:

- Public awareness campaigns seek to educate individuals about the presence of disinformation, its potential impact, and methods to recognize and counter it. Utilizing various channels, including social media, traditional media, and community events, these campaigns aim to reach broad audiences.
- Education programs go beyond surface-level awareness, aiming to develop skills such as media literacy, critical thinking, and digital citizenship. These programs provide

individuals with tools to navigate the digital landscape, critically assess information, and differentiate reliable sources from disinformation.

- Evaluation involves gauging the level of awareness within the target audience regarding disinformation. Surveys, focus groups, and analytics from online platforms offer insights into the extent to which the public is informed about the challenges posed by disinformation.
- Identifying knowledge gaps is crucial for tailoring awareness campaigns and education programs. Assessing existing knowledge and pinpointing misconceptions helps refine the content and delivery methods of educational initiatives.
- The effectiveness of these initiatives can be gauged by observing changes in behavior. Are individuals becoming more discerning in their online interactions? Are they adopting habits that indicate an increased awareness of the risks of disinformation?
- Assessing long-term impact involves determining whether the awareness and skills gained through campaigns and programs have a lasting effect. This includes observing whether individuals continue to apply critical thinking skills and share information responsibly over an extended period.
- Community engagement initiatives, such as workshops and town hall meetings, contribute to stimulating discussions and building a collective understanding of the challenge of disinformation. The impact of such engagement can be assessed through participation levels and community feedback.
- The success of awareness and education efforts often hinges on partnerships with various stakeholders, including schools, community organizations, and online platforms. Evaluating the strength and effectiveness of this cooperation is integral to assessing the overall impact.
- A combination of quantitative metrics (such as survey data and analytics) and qualitative methods (such as interviews and focus groups) offers a comprehensive understanding of impact. Quantitative metrics provide numerical insights, while qualitative methods capture nuanced perceptions and experiences.
- Continuous evaluation allows for iterative improvement. Based on feedback and emerging disinformation trends, awareness campaigns and education programs can be refined to address new challenges and maximize their impact.

Principal stakeholders, who work within information, communications, and media ecology, must be concerned about fake news, disinformation, and misinformation, and contribute to their quota in making information users more discerning with the right Media and Information Literacy (MIL) training. Social media companies must be obligated to make their users aware of fake news and disinformation and give them the necessary skills, tools, and knowledge on how to spot them. Social media companies can consider periodically asking users evaluate the accuracy of randomly sampled stories or information and providing them with the right answers afterwards. This could be a subtle but a valuable way of conscientising their users about fake news and disinformation. They can also present users with MIL tips on a regular basis.

In summary, evaluating the impact of public awareness campaigns and education programs involves a multifaceted approach considering changes in awareness levels, alterations in behavior, and the long-term sustainability of knowledge. Through a blend of quantitative and qualitative assessment methods, stakeholders can enhance strategies for building a more informed and resilient digital society. Understanding the impact of public awareness and

education initiatives is crucial for creating a more informed and resilient society against AI-driven disinformation. Analyzing changes in awareness, behavior, and the long-term sustainability of knowledge provides a foundation for improving strategies to combat disinformation. The success of these initiatives is measured not only by the initial reaction of the public but also by long-term changes in behavior and attitudes toward information. Partnerships and collaboration with different stakeholders are key to achieving a broader and deeper impact in the fight against disinformation in the digital age.

Inter-Sectoral Collaboration

Cross-sector collaboration focuses on examining the necessity of cooperative efforts among diverse entities. The effectiveness of countering disinformation campaigns relies on a coordinated effort that involves the exchange of information, the integration of diverse expertise, establishment of real-time communication channels, cooperation with law enforcement authorities, and active engagement with technology companies. In summary:

- Facilitating smooth information exchange among law enforcement, intelligence agencies, and technology companies is crucial. This cooperation optimizes the use of diverse data sets and insights, thereby bolstering the collective capability to identify and combat disinformation more effectively.
- Integration of diverse expertise is essential, bringing together insights from different sectors, including legal perspectives from law enforcement, geopolitical understanding from intelligence agencies, and technical know-how from technology companies. This ensures a thorough comprehension of the multifaceted nature of disinformation.
- The establishment of immediate communication channels is crucial for responding promptly to emerging disinformation threats. This allows for a coordinated and swift response to minimize the impact of false information before it disseminates widely.
- Engaging in cooperation with law enforcement authorities is essential for the creation and implementation of legal frameworks designed to prevent and penalize disinformation activities. This guarantees a comprehensive response that takes into account both technological aspects and legal/regulatory considerations.
- Forming partnerships with technology companies is crucial for utilizing advanced tools and algorithms effectively. This collaboration enables the application of state-of-the-art technologies in the identification, analysis, and mitigation of disinformation campaigns.

In conclusion, a holistic and collaborative approach that incorporates the strengths of different sectors is essential to effectively address the challenges posed by disinformation in the modern era. By fostering information exchange, integrating diverse expertise, establishing real-time communication, cooperating with law enforcement, and partnering with technology companies, societies can enhance their ability to identify, prevent, and respond to disinformation campaigns.

Key components of comprehensive research in this field should encompass:

- To achieve a comprehensive understanding of the aspects of human behavior and social dynamics contributing to the spread of disinformation, it is essential to examine diverse facets. The goal is to thoroughly comprehend these factors and develop strategies to mitigate their impact.
- Examine the influence of social structures, group dynamics, and interpersonal relationships in the dissemination of disinformation. This entails understanding how

false information can gain traction within echo chambers, social networks, and online communities.

- Examine cognitive biases, psychological vulnerabilities, and emotional triggers that make individuals prone to believing and spreading disinformation. A thorough understanding of these factors is crucial for developing interventions that target the root causes of disinformation consumption.
- Create educational programs with the goal of raising awareness about prevalent cognitive biases and logical fallacies. These initiatives aim to provide individuals with the skills to critically evaluate information, empowering the public to differentiate between genuine and false content.
- Implement programs that improve media literacy skills in the broader population. This includes educating individuals on how to navigate and critically assess information from diverse sources, including online platforms, traditional media, and social media.
- Advocate for the cultivation of critical thinking skills that empower individuals to question information, verify sources, and conduct contextual analyses of content. Critical thinking serves as a fundamental defense against the unintentional and intentional spread of disinformation.
- Tailor strategies to target specific social and psychological vulnerabilities identified through research. This may include designing focused interventions for particular demographic groups or online communities that demonstrate specific susceptibility to disinformation.
- Collaborate with specialists in psychology, sociology, and related fields to acquire more profound insights into human behavior. This interdisciplinary collaboration ensures a nuanced comprehension of the social and psychological factors that impact disinformation.
- Acknowledge the requirement for persistent, long-term behavior change in combating disinformation, recognizing that it goes beyond short-term interventions. This entails establishing continuous educational initiatives to foster a culture of critical thinking and media literacy.

Through systematic research and a comprehensive understanding of social and psychological factors contributing to disinformation spread, the aim is to foster the development of effective strategies. Rooted in education, media literacy, and critical thinking, these strategies seek to build a resilient and discerning public capable of navigating the intricate information landscape of the digital age.

(Zach Bastick, , 2021.) Despite the enormous threats and high risks of behavior modification through fake news, there is a paucity of controlled studies on the direct effects of fake news on behavior. New evidence shaw on the ability of disinformation to change unconscious behavior. Short exposure to disinformation (as is typical online) can have moderate effects on unconscious individual behavior, raises immediate concerns for platforms, policymakers, and social media users. These findings raise deep concerns for the future of society and politics. Disinformation risks skewing individuals' worldviews and deleteriously informing their behavior. Deliberately produced and targeted disinformation aimed at behavior modification amplifies these risks, by introducing incentives and optimization. The democratization of AI and the means of producing disinformation further amplifies these risks beyond platforms to the entire ecosystem of social media users and content. The continual efforts by malicious actors to bypass disinformation detection mechanisms implies that we must

come to terms with the existence of disinformation on social networks and be open-minded about the forms and effects of disinformation.

Conclusions

In conclusion, this study provides a foundational examination of the dynamics associated with artificial intelligence (AI)-driven disinformation and offers a comprehensive framework for addressing these challenges in the digital era. A profound understanding of the mechanisms and strategies involved in the creation and dissemination of disinformation, particularly with a focus on AI, is crucial for formulating effective strategies to minimize its impact.

By scrutinizing the social and psychological factors influencing disinformation spread, the research identifies fundamental aspects of human behavior, cognitive biases, and emotional triggers. Recognizing the necessity for the development of educational programs and initiatives in media literacy becomes imperative to enhance societal and individual resilience.

Furthermore, an AI-centric approach to disinformation detection entails the creation of advanced credibility assessment algorithms and geolocation tracking, prioritizing privacy protection. The emphasis on cross-sector collaboration underscores the importance of cooperation among legislators, technology companies, intelligence agencies, and educational institutions for a holistic response to the disinformation challenge.

The delicate task of aligning regulations with fundamental rights, such as freedom of speech and privacy, necessitates a nuanced approach. Striking a balance between countering disinformation and upholding democratic principles emerges as a crucial focal point of the research. Public awareness campaigns and educational initiatives should target long-term effects, assessing the level of awareness, behavioral changes, and the sustained proficiency of acquired skills. Ultimately, the presented framework and insights from this study contribute to the formulation of a holistic strategy for addressing the complexities of disinformation. The integration of technological innovations, education, cross-sector collaboration, and regulatory frameworks is pivotal in creating an informed, resilient, and democratic society in the digital age.

Acknowledgements. The paper is based on research conducted as part of the Erasmus+ KA220-HED project - Cooperation Partnerships in Higher Education (2022/2025).

References

1. Associate Professor Antoliš Krunoslav, PhD, professor of higher education permanent, Chief Police Adviser, member of the steering committee of the University of Applied Sciences in Criminal Investigation and Public Security, Police academy "First Croatian Police Officer", Ministry of Internal Affairs, Republic of Croatia
2. Demartini, Gianluca, Stefano Mizzaro, and Damiano Spina. 2020. Human-in-the-loop Artificial Intelligence for Fighting Online Misinformation: Challenges and Opportunities. IEEE Data Engineering Bulletin 43: 65–74.
3. Fátima C. Carrilho Santos, 2023. Artificial Intelligence in Automated Detection of Disinformation: A Thematic Analysis, by LabCom, University of Beira Interior, 6201-001 Covilhã, Portugal, Journal. Media 2023, 4(2), 679-687; https://doi.org/10.3390/journalmedia 4020043, Published: 3 June 2023

4. Graves, Lucas. 2018. Understanding the Promise and Limits of Automated Fact-Checking. Oxford: Reuters Institute for the Study of Journalism
5. Jiang, Tao, Jian Ping Li, Amin Ul Haq, Abdus Saboor, and Amjad Ali. 2021. A novel stacking approach for accurate detection of fake news. IEEE Access 9: 22626–39.
6. Kalea Texeira: Advancements in AI-Powered Threat Detection and Prevention: Enhancing Cybersecurity with Artificial Intelligence, October 20, 2023. https://www.linkedin.com /pulse/advancements-ai-powered-threat-detection-prevention-kalea-texeira-tcvec/
7. Kate Starbird, Tom Wilson, Ahmer Arif, Proceedings of the ACM on Human-Computer InteractionVolume 3 Issue CSCWArticle No.: 127 pp 1–26, https://doi.org/10.1145/3359229
8. Lilian Olivia Orero (Kenya), Balancing the protection of fundamental rights in the fight against disinformation, 21.11.2022. https://d4dhub.eu/news/balancing-the-protection-of-fundamental-rights-in-the-fight-against-disinformation
9. Nakov, Preslav, David Corney, Maram Hasanain, Firoj Alam, Tamer Elsayed, Alberto Barrón-Cedeño, Paolo Papotti, Shaden Shaar, and Giovanni Da San Martino. 2021. Automated fact-checking for assisting human fact-checkers. arXiv arXiv:2103.07769.
10. Rubin, Victoria L.: Disinformation and misinformation triangle : A conceptual model for "fake news" epidemic, causal factors and interventions, The Journal of documentation, 09 Sep 2019, Vol. ahead-of-print, Issue ahead-of-print, pages 1013 – 1034, ISSN: 00220418, DOI: 10.1108/JD-12-2018-0209, Publisher: Emerald; EMERALD GROUP PUBLISHING LIMITED, https://www.emerald.com/insight/content/doi/10.1108/JD-12-2018-0209/full/html
11. The paper is based on research conducted as part of the Erasmus+ KA220-HED project - Cooperation Partnerships in Higher Education (2022/2025).
12. Theodora Dame Adjin-Tettey (2022) Combating fake news, disinformation, and misinformation: Experimental 1 Theodora Dame Adjin-Tettey (2022) Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education, Cogent Arts & Humanities, 9:1, DOI: 10.1080/23311983.2022.2037229
13. Westlund, Oscar, Rebekah Larsen, Lucas Graves, Lasha Kavtaradze, and Steen Steensen. 2022. Technologies and Fact-Checking: A Sociotechnical Mapping. In Disinformation Studies. Covilhã: Beira Interior University, p. 193.
14. Zach Bastick, Would you notice if fake news changed your behavior? An experiment on the unconscious effects of disinformation, Computers in Human Behavior, Volume 116, 2021, 106633, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2020.106633. evidence for media literacy education, Cogent Arts & Humanities, 9:1, DOI: 10.1080/23311983.2022.2037229