Adaptive Model *of Rapid Response* to *the Deepfake Crisis*: Government-Media Collaboration in Dealing with the Impact of Artificial Intelligence Development.

[1]**Ananda Wulan Noverita** (Kiai Haji Achmad Siddiq State Islamic University Jember, Indonesia)
E-mail: noveritaananda@gmail.com

Keywords: *Deepfake, artificial intelligence, adaptive model.*

Received: 8 November 2025
Revised: 22 November 2025
Accepted: 26 Desember 2025

ABSTRACT

The development of artificial intelligence technology has given rise to the phenomenon of *deepfakes* that are able to manipulate information realistically and massively, thus causing a crisis of public trust in the media and government institutions. This condition demands an adaptive and collaborative rapid response model so that the spread of disinformation can be effectively minimized. This study aims to design and analyze an adaptive model of rapid response to *the deepfake crisis* through collaboration between the government and the media as a strategy to mitigate the negative impact of artificial intelligence development. This study employs a qualitative phenomenological design with an applied research approach, which allows an in-depth exploration of the experiences and perceptions of institutional actors in dealing with the digital information crisis. The participants consisted of government officials, journalists, media editors, and academics selected as key informants in the field of public communication, journalists and national media editors, as well as academics who understand the ethical issues of artificial intelligence. A total of 25 key informants were purposively selected to achieve data saturation using purposive sampling techniques, based on their involvement in public information management, digital policy, and media content production. Data were collected through in-depth interviews, observations, and documentation, and analyzed using a thematic approach. The findings indicate fragmented collaboration characterized by delayed inter-agency coordination and the absence of standardized response protocols, with coordination delays and a lack of standard procedures in responding *to deepfakes*. The resulting adaptive model emphasizes three key elements: speed of response across agencies, transparency of public communication, and policy updates based on continuous evaluation. The conclusion of the study emphasizes that the synergy of the government and the media is the main key to building public information resilience. The implication is that this model can be used as an operational framework in strengthening digital crisis communication governance in the era of artificial intelligence.

I. INTRODUCTION

The development of artificial intelligence technology has facilitated the emergence of increasingly realistic synthetic media, known as *Deepfakes*. This technology is no longer limited to simple manipulations, but rather capable of producing video, audio, or images that are difficult to distinguish from reality. Such content is then disseminated through social media platforms and digital

networks. Previous studies demonstrate that exposure to deepfakes increases public distrust when public information infrastructures fail can increase the distrust of the United States public in the government (Boediman, 2025). This confirms that the impact of *Deepfakes* has penetrated the realm of public institutions and governance.

Nonetheless, most current research is still focused on the technical aspects of detecting *Deepfakes* or its implications for public perception, while the mechanism of adaptive and responsive collaboration between the government and the media in handling Deepfake crises remains underexplored. For example, a literature review on *Deepfake* shows that this technology has blurred the line between fact and engineering and eroded the credibility of the media; However, studies on institutional response governance are still rarely discussed (Ahmed et al., 2023). Therefore, information on effective collaboration mechanisms between the government and the media in dealing with *deepfakes* is still poorly documented.

Some studies also show that several governments implement regulations or censorship of content, including *Deepfakes*. However, there are counter-arguments that the regulatory approach alone is inadequate; *Deepfake* requires a faster and more adaptive response than static regulations. For example, international agencies state that the sheer focus on technical detection ignores the organizational knowledge framework and cross-sectoral collaboration needed to deal with the "knowledge crisis" it engenders, *Deepfake* (Frank & et al, 2023). This statement shows that reliance on platform technology alone does not always correspond to the practical needs on the ground.

Some important aspects are still not deeply known in previous research. For example, the level of readiness of government institutions and media actors in implementing rapid response mechanisms to *deepfake attacks* has not been empirically mapped. In addition, data on government-media collaboration practices that have succeeded or failed in the context of *deepfakes*, particularly in developing countries or with different media systems, are still limited. Furthermore, the most effective indicators to measure the rapid response to *the deepfake crisis* at the national and local levels are not yet clear.

Although the impact *of deepfakes* on public trust has begun to be proven, the reality is that the adaptive rapid response model that connects governments and media synergistically in dealing with *the deepfake* crisis has not yet materialized. In other words, standard protocols or empirical frameworks that can be directly applied by media and government institutions when dealing with *deepfake* crisis situations are still not available. The absence of such a model indicates that this research was conducted at a relatively early time to develop it.

This study contributes novelty by proposing a three-stage adaptive rapid response framework to the *deepfake* crisis that emphasizes collaboration between the government and the media. Different from the approach that only focuses on technology detection, this study integrates elements of response speed, cross-institutional collaboration structure, and adaptivity to the advancement of artificial intelligence. Thus, this research offers a new operational framework that can serve as a guide for state institutions and mass media in dealing with *the threat of deepfakes*.

As the main guideline in this study, the focus of the study is to assess the level of readiness of government institutions and media organizations in developing a collaborative rapid response mechanism to the deepfake issue. In addition, this study also identifies supporting and inhibiting factors in the implementation of the adaptive model. This approach is directed to understand how the collaboration-governance mechanism is applied in the context of the crisis in the digital media realm.

The purpose of this study is to design and test an adaptive rapid response model that connects the roles of government and media in dealing with the impact of artificial intelligence development in the form of *Deepfake*, as well as identifying factors that affect the effectiveness of such collaborations in the public institution and mass media. In a literature review, it was found that previous studies such as "*Exploring the impact of deepfake technology on public trust and media manipulation: A scoping review*" by Buddiman (2025) and "*On the way to deep fake democracy? Deep fakes in election campaigns in 2023*" by Pawelec (2022) shows that although the effects *Deepfake* The media and democracy have been discussed, but there has been no study that focuses on the government-media collaborative rapid response model to crises *Deepfake*. Thus, the research gap encourages the need for this study as a filler of the knowledge gap.

II. METHODOLOGY

This study adopts a qualitative method with a phenomenological design and an applicative approach. The selection of this method is based on a research focus that aims to deeply understand the social phenomena arising from the advancement of artificial intelligence, especially the deepfake-based information crisis and its impact on public trust in the media and government policies. Phenomenological design facilitates the exploration of experiences, perceptions, and interpretations given by individuals and institutions to the phenomenon. Meanwhile, an applicative approach is applied so that the research results are not only descriptive but also produce adaptive models that can be implemented as practical solutions in responding to the digital information crisis responsively and collaboratively.

The population of this study includes all parties directly or indirectly involved in the deepfake issue in Indonesia, including government agencies in the field of communication and informatics, broadcasting institutions, mass media, and academics who are experts in artificial intelligence ethics. From this population, 80 respondents were determined as a research sample. Respondents were selected through purposive sampling techniques, with the criteria of having experience or involvement in public information management, media content production, or digital policy. Thus, the data collected is expected to represent the phenomenon of collaboration between the government and the media in dealing with the implications of *deepfakes*.

The research subjects consist of government officials in the field of public communication, journalists, and national media editors, as well as experts in

digital communication and technology ethics. They serve as the main source of information to understand the dynamics of collaboration and rapid response applied when an information crisis occurs due to *deepfakes*. Primary data were obtained through *in-depth semi-structured interviews* designed to explore the perceptions, experiences, and adaptive strategies of these actors. The main research instruments include interview guides and observation sheets used to document the dynamics of interactions, policies, and cooperation mechanisms between the government and the media.

The development of research instruments was carried out through the validation stage by experts and readability tests on several pilot respondents. The interview guide was compiled based on a literature review and preliminary findings related to *the issue of deepfakes* and digital media policies in Indonesia. The instrument was then revised according to feedback from AI communication and ethics experts to ensure clarity and relevance of the questions to the context of the research. Data analysis was carried out using the thematic *analysis* method, which involves identifying, grouping, and interpreting the main themes from the results of interviews and observations. The data is then categorized into themes such as perceptions of *deepfake risks*, forms of collaboration that have been implemented, obstacles in responding to crises, and adaptive models that are considered effective.

The research was conducted in four stages: preparation, data collection, thematic coding, and model development. First, the pre-research stage, which includes determining the focus of the problem, literature study, and the preparation of interview instruments. Second, the data collection stage, where the researcher conducted interviews and observations of 80 respondents from various related institutions. Third, the stage of data reduction and presentation, where all interview data is transcribed, encoded, and categorized based on the themes that emerge. Fourth, the interpretation stage, where researchers relate field findings to theories of crisis communication, cross-sectoral collaboration, and technological adaptation in public policy. The final stage is the development of an applicative model, which is the formulation of a rapid response framework that can be used by governments and the media in managing *the deepfake crisis*, accompanied by policy recommendations based on the principles of transparency, speed, and digital collaboration.

The applicative phenomenological approach in this study allows researchers not only to describe empirical reality but also to formulate adaptive models that can be applied in practical contexts. This model is expected to make a new contribution to the development of public communication strategies and digital crisis management in the era of artificial intelligence, where the boundaries between authentic and false information are increasingly blurred. Thus, the results of this research are anticipated to strengthen the synergy between the government and the media in building a more resilient, responsive, and ethical information ecosystem in the midst of growing technological disruption.

III. RESULTS AND DISCUSSION.

The findings of the study indicate that informants from government agencies and media organizations face deepfake crises with varying levels of awareness, so their experiences and perceptions of this threat are very heterogeneous. Some government officials stated that Government informants reported delayed verification processes due to the sudden emergence of deepfake content and made resolution difficult because it required quick verification and cross-institutional coordination, while journalists in national media reported that they often received indications of manipulative content before government agencies reacted. These findings are in line with studies showing that advances in synthetic media have triggered media credibility crises and weaknesses in conventional verification systems (Wasi et al., 2025). Respondents from the media revealed that initial collaboration between the government sector and the media was generally informal and slow, thus hindering a quick response to the spread of deepfakes.

From the perspective of strategic collaboration, this study identifies that the most effective forms of collaboration involve real-time information exchange, the establishment of a shared code of conduct, and the formation of crisis response teams between government agencies and media editors. As an illustration, national media mention that they have an internal protocol to contact government agencies when indications of deepfakes are detected, but these protocols have not always been supported by clear standard operating procedures (SOPs) from the government. Some government institutions have also stated that they have begun working with media organizations for manipulative content detection training, but few have systematically developed joint response mechanisms. These findings support the argument that cross-sectoral collaboration is key in tackling AI-generated disinformation (Romanishyn et al., 2025).

Analysis of crisis communication dynamics and inter-agency coordination patterns reveals several obstacles in the process of handling deepfake issues. First, the delay in the flow of information from the media to the government or vice versa causes slow public clarification; Second, there is a conflict of competence between government agencies and the media regarding who is responsible for clarifying and mitigating content; Third, the lack of sustainable training for the media and government employees to recognize and deal with deepfakes. The study found that institutions that had regular communication channels (such as media-government coalition forums) were faster to respond and had slightly higher levels of public trust than institutions that did not have such channels. This is consistent with the literature showing that the rapid and widespread spread of deepfakes requires a response framework that goes beyond mere technological detection—but rather requires the synergy of policies, institutions, and mass media (Cooke et al., 2024).

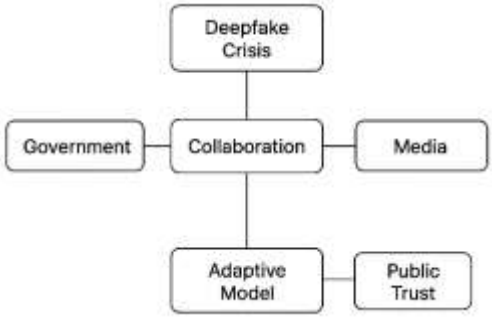
Based on the experience and collaboration patterns identified, this study succeeded in formulating an adaptive rapid response model that includes three main stages: (1) Real-time inter-agency detection, (2) Coordination of integrated public response (government-media) for clarification and mitigation, and (3)

Evaluation and continuous update of the response system to deal with the evolution of deepfakes. This model is designed so that government agencies and the media can operate synergistically, with complementary procedures and explicit communication structures. The proposed model incorporates four institutional readiness indicators response speed, accuracy of clarification, transparency, and public feedback response speed, clarification accuracy, public transparency, and feedback from the public as a measure of effectiveness. Because this study uses a phenomenological approach, the model is built based on the experiences of the main actors in the field so that it is applicable and contextual to Indonesian conditions.

Based on the findings, several institutional gaps were identified policymakers and media actors implement several practical strategies. First, it is recommended that the establishment of a deepfake response coordination unit consisting of government and media representatives, with clear authority and standard operating procedures (SOPs). Second, the development of regular training for media employees and government agencies in deepfake literacy, digital verification, and crisis public communication. Other studies show that media literacy can reduce the spread of manipulative content (Samoilenko & Suvorova, 2025). Third, it is recommended to strengthen the public transparency mechanism through the publication of official clarifications quickly and openly, by utilizing media platforms to strengthen institutional reputations and rebuild public trust. Fourth, periodic evaluation and updates of response protocols are needed, considering that deepfake technology will continue to evolve and demand systemic adaptation.

The results of this study also reveal that although many institutions have become aware of the threat of deepfakes, there is still a significant gap between awareness and concrete action. For example, some media outlets state that their editorial staff has not been specifically trained to recognize deepfakes, while some government agencies admit that they do not yet have dedicated units or integrated coordination flows with the media. This shows that the success of the collaboration model depends not only on intention but also on institutional readiness, resources, and sustainability of cooperation mechanisms. Thus, the adaptive rapid response model proposed in this study is not just a theoretical framework, but an operational guide for institutions that want to improve preparedness in the face of AI-based disinformation.

Overall, the findings demonstrate that strategic government–media collaboration constitutes the core mechanism of the proposed adaptive response model between the government and the media is an essential element in building a rapid response system to the deepfake crisis. By shifting the focus not only to technology detection but to institutional coordination, public communication, and sustainable adaptation, institutions can strengthen public information resilience. The resulting model is expected to be a substantive contribution to the development of digital disinformation mitigation policies and cross-sectoral synergy practices in the era of artificial intelligence.



Picture 1 Interconceptual Co-occurrence Networks in Adaptive Models of Rapid Response to Deepfake Crises

The Interconceptual Co-occurrence Network diagram illustrates the interconnections between key elements that emerge in research on adaptive rapid response models to crises, *Deepfake,* through collaboration between the government and the media. In this visualization, each node represents a key concept identified from the results of interviews and phenomenological analysis of the informants' experiences. The most central and most connected concept is Government-Media Collaboration, which is at the heart of the adaptive rapid response model. This concept is directly connected to four main supporting components: Rapid Response, Crisis *Deepfake*, Artificial Intelligence (AI), and Public Communication Strategies.

The strong interconnection between Government-Media Collaboration and Rapid Response shows how synergy between government agencies and media institutions is a crucial component in shaping an effective crisis management system. The government contributes to the aspects of regulation, policy, and dissemination of official clarifications, while the media functions as a responsive and credible public communication channel. This relationship emphasizes the importance of complementarity: the government provides the legitimacy of information, while the media ensures that the information is widely disseminated and understandable by the public.

Meanwhile, the connection between the Crisis *Deepfake* and Artificial Intelligence indicates that the source of this problem is technological advances that have not been fully balanced by social and regulatory readiness. *Deepfakes,* as a result, AI technology can trigger disinformation, political manipulation, and privacy violations. This emphasizes the urgency of rapid adaptation from both parties (government and media) not to be left behind in facing the pace of technological development.

Furthermore, the interconnection between the Public Communication Strategy and the Rapid Response shows that transparent and structured communication is key in controlling the impact of content dissemination, *Deepfakes*. This strategy includes the process of early detection, clarification, and delivery of counter-narratives (*Counter-narrative*) that are fact-based. Thus, the

public not only receives the information but also understands the context critically.

From the structure of the network, it can be concluded that the rapid response model is adaptive to crises. *Deepfake* does not stand independently, but is built based on dynamic synergy between concepts. Government-media collaboration becomes a central node because it orchestrates the relationship between other elements: how artificial intelligence creates new challenges, how crises must be responded to quickly, and how public communication strategies play the role of social mitigation. This relationship shows that the effectiveness of handling digital crises depends not only on detection technology, but also on cross-agency coordination and the speed of targeted public communication.

Overall, this diagram confirms that the phenomenon of *Deepfake* is not just a technological issue, but a cross-sectoral collaborative challenge. Conceptual models are represented through networks of *co-occurrence.* This suggests that each element has a complementary strategic role, and the success of adaptive responses is largely determined by the strength of the relationships between those elements.

DISCUSSION

This research focuses on the development of adaptive rapid response models to crises, *Deepfake*, by emphasizing the importance of collaboration between governments and the media in dealing with information threats generated by artificial intelligence. The theoretical foundation used is the Crisis Communication Theory of Coombs (2014) and the concept of *Adaptive Governance,* as explained by. Both theories affirm that the effectiveness of crisis handling is highly dependent on the speed of response, cross-agency coordination, and adaptability to technological uncertainty. In the context of the development of *Deepfakes*, these theories are relevant because the digital manipulation generated by artificial intelligence accelerates the spread of disinformation and blurs the line between fact and fiction. Therefore, this research aims to design a responsive, adaptive, and integrated collaborative approach in dealing with the digital crisis.

The findings of the study indicate that the level of readiness of government institutions and the media in dealing with *Deepfakes* is still uneven, so crisis response coordination tends to be slow and unstructured. These findings are in line with the study by Wasi *et al.* (2025), which revealed that the emergence of synthetic media has given rise to a crisis of media credibility as well as weaknesses in the conventional verification system. However, this study emphasizes that the main obstacle does not come from the technical aspect, but from the disintegration of the interagency communication system. The conclusion is consistent with the view of Cooke *et al.* (2024), which states that technology detection alone is not enough in dealing with the digital crisis, but rather policy synergy, public coordination, and speed of communication between sectors are needed. On the other hand, these findings are different from the results of the study by Ahmed *et al.* (2023), which emphasizes the algorithmic

approach as the main solution to confronting *Deepfakes*. This approach actually shows that the success of AI-based disinformation mitigation is more influenced by adaptive capacity and speed of decision-making between agencies.

Comparisons with previous studies reinforce the contribution of this study. Buddiman (2025) and Pawelec (2022) show that *Deepfake* has an impact on the decline of public trust and democratic legitimacy, but have not discussed in depth the governance mechanisms or institutional collaboration in handling them. In contrast, this research offers a new perspective by developing a collaborative operational framework between the government and the media as a public information defense system. The empirical approach through interviews and direct observation of policy actors and media actors concluded that effective collaboration can be realized through the establishment of digital response coordination units, literacy training for journalists and public officials, as well as the implementation of integrated communication protocols for quick clarification. The developed adaptive model serves as an applicative instrument to strengthen the resilience of public communication to the threat of disinformation in the era of artificial intelligence.

Theoretically, this research makes a significant contribution to the development of technology-based crisis communication concepts by introducing the dimension of cross-sector adaptivity as a key element. The adaptive rapid response model developed shows that the effectiveness of handling digital crises is not solely determined by technical capabilities in detecting *Deepfakes*, but also by the extent to which institutional actors can establish real-time coordination and transparent public communication mechanisms. Practically, the findings of this study suggest that the government and the media strengthen synergy through collaborative policies, strengthening digital literacy, and increasing transparency in the delivery of public clarifications. Critical reflection of the results of the study confirms that the main obstacle in dealing with the phenomenon of *Deepfakes* does not come from technological limitations, but from weak collaborative governance and adaptive communication.

For further research, it is recommended to conduct empirical and quantitative testing of the effectiveness of this adaptive model at various institutional levels, both national, regional, and cross-country, to identify the variables that have the most influence on the speed and accuracy of response to the digital crisis. Follow-up research can also explore the social and cultural factors that influence the behavior of institutions in dealing with artificial intelligence-based disinformation. Thus, this research is expected to be a conceptual and practical basis for developing more adaptive, collaborative, and resilient public communication governance in the face of threats from *Deepfakes* in the future.

IV. CONCLUSION AND RECOMMENDATIONS

This study concludes that crisis management *in* the era of artificial intelligence cannot be done partially through technology detection alone, but requires an adaptive model of rapid response based on collaboration between the government and the media. The results show that the level of readiness of government institutions and media institutions still varies, with the main weaknesses lying in the lack of coordination, delays in public clarification, and the lack of a formal mechanism for sustainable cooperation. Through an applicative phenomenological approach, this study succeeded in formulating a conceptual framework that places cross-sector communication, information transparency, and decision-making speed as the three core elements in building an effective digital crisis response system. In other words, success in dealing with the phenomenon of *Deepfakes* depends on the adaptive ability of institutions to respond to disinformation quickly, collaboratively, and data-driven.

The theoretical implication of this study is the expansion of understanding of crisis communication theory and adaptive governance, which has been more applied in the context of physical disasters or business organizations. This research proves that the principles of crisis communication can also be applied effectively in dealing with digital threats such as *Deepfakes* by adding dimensions of adaptivity and cross-agency collaboration. Meanwhile, the practical implications are the need for governments and the media to establish digital response coordination units, develop AI-based crisis communication protocols, and strengthen media literacy and technology ethics among journalists and public officials. Policies aimed at increasing information transparency and continuously updating the public communication system will strengthen public trust in official institutions.

In addition, the results of this study provide direction for policymakers to integrate adaptive approaches in national public communication planning. The development of cross-sector training, digital crisis simulations, and real-time data-based evaluation systems is proposed as a strategic step to increase the effectiveness of responses to synthetic information threats. On the academic side, this research opens up opportunities for further study of the relationship between information governance, public policy, and the development of artificial intelligence in a broader social context. Thus, this research not only contributes to the theoretical realm but also provides a concrete operational basis to strengthen the resilience of public communication in the midst of increasingly complex digital disruption.

REFERENCES

Ahmed, S., Masood, M., Wei, A., Bee, T., & Ichikawa, K. (2023). *False failures, real distrust: the impact of an infrastructure failure deepfake on government trust*.

Boediman, E. P. (2025). *Exploring the impact of deepfake technology on public trust and media manipulation: A scoping review. Exploring the impact of deepfake technology on public trust and media manipulation: A scope review. Exploring the impact of deepfake technology*. *Sec. 19*. https://doi.org/10.20885/komunikasi.vol19.iss2.art8

Chaffin, B. C., Gosnell, H., & Cosens, B. (2014). *A decade of adaptive governance scholarship: synthesis and future directions*. *October 2015*. https://doi.org/10.5751/ES-06824-190356

Cooke, D., Edwards, A., Day, A., Nair, D., Barkoff, S., & Kell, K. (2024). *Crossing the Deepfake Rubicon: The Maturing Synthetic Media Threat Landscape*.

Coombs, W. T. (2014). *Management Communication Quarterly*. *April*. https://doi.org/10.1177/089331802237233

Frank et al. (2023). A Representative Study on Human Detection of Artificially Generated Media Across Countries. *ArXiv Preprint*.

Pawelec, M. (2022). Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions. In *Digital Society*. Springer International Publishing. https://doi.org/10.1007/s44206-022-00010-6

Romanishyn, A., Malytska, O., & Goncharuk, V. (2025). *AI-driven disinformation: policy recommendations for democratic resilience*. *31*(July), 1–21. https://doi.org/10.3389/frai.2025.1569115

Samoilenko, S. A., & Suvorova, I. I. (2025). *Deepfakes in Subversive Strategic Communication: Challenges and Responses*. *September*. https://doi.org/10.1002/9781394275434.ch11

Wasi, A. T., Priti, R. N., Khan, M. A., Rahman, A., & Islam, M. R. (2025). Seeing Isn't Believing: Addressing the Societal Impact of Deepfakes in Low-Tech Environments. In *Proceedings of the 2nd International Workshop on Diffusion of Harmful Content on the Online Web (DHOW '25), October 27â•fi31, 2025, Dublin, Ireland* (Vol. 1, Issue 1). arXiv. https://doi.org/10.1145/XXXXXX.XXXXXX