INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com
Volume 2, Issue 1 (2024)

Deepfake Deterrence: can Ai-generated Bluffs Undermine Pakistani Nuclear Credibility?

Shah Faisal, Nowroz Khan

Shah Faisal
Bacha Khan University Charsadda
Email: faisal_shahg19@gmail.com

Nowroz Khan
Bacha Khan University Charsadda
Email: khan_torangzai@gmail.com

Abstract
This paper looks at the possibility of deepfakes through AI to discredit the reputation of the Pakistan nuclear deterrence rule. Deepfakes as an example of AI-generated material with the potential to produce hyper-realistic and artificial media have emerged as a less than ideal feature of national security and geopolitical stability. In that particular study, the impacts of deepfake on Pakistan nuclear posture are under scrutiny since it forms a crucial component of its security policy. The paper also seeks to comprehend the vulnerability of these technologies in being used to perpetrate hoax nuclear threats or misinformation that may affect the strategic credibility of Pakistan. The study adopts the mixed-methods approach in which the quantitative data collected through the analysis of social media and qualitative data through interviews of the security analysts and policymakers is used. These results indicate that although there is a possibility that deepfakes will affect the understanding of nuclear threats, the credibility that Pakistan already developed in relation to nuclear weapons, basing on its history and strategic communication, is strong. The increasing complexity of AI is however, the new threat to the international policies. The study adds its voice to the debate on the nexus of cybersecurity, nuclear security, and technological development in international relations as it urges all the stakeholders to improve their knowledge and preparedness regarding dealing with the challenges posed by AI.

Keywords: Deepfakes, nuclear deterrence, media generated by Artificial intelligence, Pakistan, disinformation, the national security, geopolitics stability, and construction

Introduction
The success of artificial intelligence (AI) has been an incredible change in a number of domains, such as military and warfare, information warfare, and national security. Deepfakes are among the most disruptive AI technologies: highly realistic, synthetically generated pieces of media that are produced by using machine learning technologies, such as Generative Adversarial Network (GANs). Deepfakes are capable of producing fake content, be it in the form of videos, audio, or images that are hard to differentiate between authentic media by the viewers. This exploitation of

digital media has been rattling alarm bells in several arenas particularly as far as the field of national security and approaches to nuclear deterrence are concerned.

Deepfakes are a new problem in information war. They present an opportunity to change the perception among citizens, give a wrong impression to decision-makers, and form narratives that are not factual. The countries such as Pakistan, where nuclear deterrence has become one of the central aspects of national security, have something to lose tremendously. Deterring using nuclear weapons depends not solely on the capability of owning the weapons but the capability to convey their credible threats to the adversaries. Credibility of the nuclear deterrence measures is crucial in creating peace, particularly in highly fragile areas where the world is likely to experience conflicts among nations, e.g. South Asia, which sees a continuous tussle between Pakistan and India in relation to their nuclear rivalry. The research problem here revolves around learning how deepfake technology can destroy this credibility especially when it is applied in creating nuclear threats or even erroneously reporting on military activities.

In discussing the importance of nuclear deterrence, strategic ambiguity and articulate communication have a paramount importance in a way that cannot be surpassed. The use of nuclear deterrence is based on the belief that a state actually possesses the ability to respond and can do so with massive power to aggression. Being misinterpreted or deepfaked by the media, a fake signal to the opposition could cause confusion with regard to a nuclear posture that could easily result in the costly escalation and/or unintended miscalculation.

The importance of the given research to the sphere of the international relations, nuclear security, and digital misinformation is exponentially increasing. The emerging latest technological advancements point to the fact that deepfakes technology has become more sophisticated and capable of creating geopolitical imbalance in relationships. Chesney and Citron (2019) state that the technology of deepfake can be applied in disinformation campaigns, whereby false information, i.e. a simulated nuclear explosion or military exercise, might be curated to influence people or may lead to an international conflict. This is not only imperative to national security but especially the aspect of nuclear deterrence where perception and credibility may come in handy.

Over the last couple of years deepfakes have caught the attention in various spheres such as politics, election security, and media. To illustrate, in the 2020 Presidential elections in the United States, there was worry among some quarters that deepfakes could be used to influence the behavior of voters or smear the image of candidates (Franks et al., 2020). The fact that nuclear security is more at stake is also more urgent since misinformation in the nuclear plane can lead to disastrous outcomes. The possibility of the deepfakes to stage nuclear crises or military provocation may lead to the erosion of international trust in nuclear deterrence plans and destabilize the state of security conditions.

This study is motivated by a number of new trends in the domains of digital misinformation, nuclear security and international relations. To begin with, it can be stated that the swift progress of AI technology, especially regarding the creation of deepfakes, poses an issue about the fact such

technologies create new security risks to national security. The Deepfake technology has never been more available, as it allows an individual or a group (state or non-state actors) to produce complex media to fool scores of people. The capacity to create such media has massively surpassed the effort to come up with the technology of detection thus governments and international bodies are finding hard to match the speed of innovation.

Second, the increased popularity of social media as one of the most common mediums of information delivery has increased the potential of deepfakes. However, in contrast to traditional media, the dissemination and delivery of potential content are more controlled in social media, which is why dissemination is easy and swift and this issue is hard to control after spreading disinformation becomes possible. This is especially worrying during the issue of nuclear deterrence whereby news about nuclear capability of a state should be delivered in an effective and clear manner to create deterrence effectiveness.

Third, the present study is necessary because of the increasing tensions in South Asia, and most specifically, between the nuclear-equipped countries such as India and Pakistan. The stakes behind misinformation are high in this volatile region and the loss of credibility of the deterrence through nuclear weapons would have disastrous consequences. Since the Pakistan nuclear policy is founded on strategic ambiguity, the possibility that deepfakes are used to transform the understanding of the Pakistan nuclear policy becomes a risk that cannot be overlooked. Due to the skills of deepfakes to replicate provocative acts, like a nuclear test or an army deployment, there was the potential to add the fuel to a fire in an already aggressive part of the world or, on the extreme, escalate the situation to the point of miscalculation.

Literature Review

Employment of artificial intelligence (AI) and its effect on international security caused massive changes in world relations and approaches to military development. One such technology is deepfake, a hyper-realistic media, artificially generated by AI, that can emulate human beings, voices, and events in a realistic way, and which has already manifested itself as a disruptive technology, especially in the field of national security. In analyzing the tip of the iceberg of the research on nuclear deterrence, the deep fake, and the frenzy between digital misinformation and nuclear security, this literature review takes a look at the current extent of the research on the aforementioned three topics. It also points out seminal research, recent developments, research tools employed in comparable researches, and the research gap to be filled in this study.

The idea of nuclear deterrence has been the basis of military and political strategy over a period of decades. Earlier studies on nuclear deterrence by the likes of Schelling (1960) the Strategy of Conflict as well as Jervis (1978) Perception and Misperception in International Politics examined the psychological and communicative aspects of nuclear deterrence in terms of how credible threats and strategic ambiguity help to keep the situation at bay. These works contended that nuclear deterrence strategy effectiveness does not only hinge on the availability of nuclear devices but rather on the persuasiveness of a state to use these instruments in retaliation of aggressions.

The former ones, however, call into question these familiar concepts of deterrence, as newer technologies, e.g. deepfakes, are emerging. The potential political use of deepfakes has been discussed as the instrument of computational propaganda and manipulative political campaigning, cyber warfare (Franks et al., 2020). It is tested in the context of misinformation and its possible effects on democratic institutions, voting procedures, and international affairs because the technology allows generating fake media with Generative Adversarial Networks (GANs) (Chesney & Citron, 2019). Although a lot of research has been devoted to the issue of deepfake detection and to how AI in media is potentially unethical (Boulton, 2018), not much has been done to study how AI in media is likely to impact the nuclear deterrence.

The modern breakthrough in the field of AI generated a new wave of considering the importance of digital misinformation as something capable of affecting security policies and national defense strategies. By way of illustration, deepfake technology might replicate the showcasing of a nuclear crisis/military action that would cause misperceptions among other states/population (Katz, 2019). There is danger of escalatory measures being undergone because of this manipulation of information and it destroys stability that the old school nuclear deterrence strategies used to give. Consequently, researchers such as Jaspal (2020) have started considering the importance of digital misinformation in nuclear security yet the research on how such technologies might interfere with particular strategies (e.g., strategic ambiguity) used by states like Pakistan to sustain nuclear deterrence is still in the early stages.

Past research related to the integration of AI and security has applied different methodology and research interests have concentrated on the use of machine learning algorithm, sentiment analysis, and natural language processing (NLP) to interpret online content. In another example, Franks et al. (2020) applied machine learning techniques to study how deepfake videos go viral and attract user consumption in the social media. On the same lines, Chesney and Citron (2019) have used the legal and policy analysis lenses to discuss the consequences of the deepfake material on democracy and national security. Although these studies give essential information about the dangers of deepfakes, very little attention has been given to the impact of deepfakes in terms of addressing nuclear deterrence, or how deepfakes can be employed to weaken national security measures.

Major Findings

A number of articles have noted how deepfakes have the capacity to affect the international relations and the national security. Franks et al. (2020) stated that deepfakes may also be utilized to construct fake reports or start a conflict by faking important diplomatic or military messages. The results of their surveys indicate that the issue of deepfakes poses a growing risk to the global relations, especially when the stakes are high (as in the case of nuclear diplomacy). Chesney and Citron (2019) also pointed to the dual threat of deepfakes, as they play a potential role in a breach of critical infrastructure and fraudulent use of military communication channels, in addition to subverting the perception of the population.

The takeaways of these studies can be understood in a clear way: deepfake technology can be used

to create an atmosphere of uncertainty, an environment in which decision-makers do not know anymore which signals they receive are authentic, and which ones are fabricated. Such an uncertainty in the nuclear context may undermine the strength of deterrent posture of a state. According to Jaspal (2020), misinformation could start in the nuclear field resulting in possible misinterpretation and in a worst-case scenario, an accidental conflict escalation.

Although the interest towards the deepfake technology increases, there is still no researched field concerning the influence of this phenomenon in the nuclear deterrence field. The available literature has paid a lot of attention to the legal and political effects of deepfakes but has overlooked the likely detrimental implication of the technologies on strategic military doctrines, especially those anchored in strategic ambiguity. Additionally, in spite of the increasingly growing activity in the studies of AI and its role in geopolitics, as in a study by Franks et al. (2020), that study is only conducted on the general effect of the AI in geopolitics but there is a lack of research in terms of how deepfakes can specifically distort perceptions of nuclear threats or create a shift in the credibility of nuclear deterrence strategies.

This study will fill in these research gaps by looking at the potential effect of deepfakes on Pakistan nuclear deterrence effect specifically, which is based on strategic ambiguity and message transmission of the nuclear threats. It also addresses the general impacts of the deepfake technology on nuclear stability in the world and how such danger may be curbed in terms of international collaboration and cybersecurity.

This paper further enhances previous studies on the use of deepfakes by narrowing down to look at one national security strategy i.e. nuclear deterrence by Pakistan and how the strategy would be destroyed by deepfakes. This research will investigate the issue from the perspectives of both quantitative analysis of social media and qualitative interviews with experts that will provide a more in-depth insight into the problem.

Significance

The relevance of the study lies in the fact that it is an unexplored issue in the grouping of technology, national security, and international relations. Online malinfo, especially those generated by artificial intelligence in the form of deepfakes, is an increasingly troubling issue to nuclear deterrence, which is a pillar of peace and stability in the globe. By examining the case of Pakistan, which is a major nuclear state in South Asia, this paper will offer a reflection of how digital manipulation might destabilize the nuclear activities in the region, which normally faces a strain in the geopolitical sphere.

Research Objective

The main goal of the given study is to identify the possible influence of deepfake technology on the viability of Pakistani nuclear deterrence policy. This paper will take the following aim:

1. In what manner, deepfakes could be used to prove nuclear capabilities or military acts on the behalf of Pakistan.
2. Find out what some experts have to say about how the nuclear strategy of Pakistan can withstand

the attacks of deepfake technology.
3. Inquire about the policy implications of the Pakistani security strategy and nuclear stability of the world.

Research Questions

1. What are the ways the deepfake technology can be applied to changing the perceptions of the nuclear capabilities or threats that Pakistan poses?
2. What can the presence of deepfakes mean with regard to the strategic ambiguity employed by Pakistan regarding the nuclear deterrence?
3. What are some of the steps that Pakistan can take in order to better their cybersecurity and global partnerships to reduce the threats presented by deepfakes?

Theoretical Framework

The theoretical framework of this study includes the theory of nuclear deterrence and specifically the strategic ambiguity theory along with misinformation theory on digital and cybersecurity. The article addresses the issue of the power of deepfake technologies against conventional frames of deterrence arguments of the credibility of nuclear threats and information instability in which these threats are conveyed. It also uses information warfare theories that highlight strategic analysis of digital technologies to exert influence over people who seek to manipulate perceptions and decision-making process in high-stakes situations.

Methodology

The research also uses mixed methods to conduct an assessment of how deepfake technology could affect the nuclear deterrence credibility in Pakistan. The mixed methodology of using both quantitative data analysis and qualitative insights will help to give the study a more comprehensive scope on the effects that AI-generated media can have on the view of nuclear threats and on the feasibility of its effects on national security, in general. The same methodological underpinning can not only provide a means of inspecting empirically the nature of pubic opinion and media propagation but can also provide qualitative knowledge and opinion of those with expert knowledge on the subject of security and nuclear deterrence.

Research Design

The research is based on a sequential explanatory design as a typical mixed methods methodology that is applied in social science research and that is especially successful when there is a focus on explaining an intricate phenomenon (Creswell & Clark, 2017). The construction starts with the quantitative analysis of the social media data with the specific purpose of analyzing interactions in deepfake material associated with the issue of nuclear threats. This would be supplemented by use of qualitative research involving semi-structured interviews with policymakers, security experts, and military strategists with a view of gaining in-depth information on the issues of concerns and perceived threats to the nuclear credibility of Pakistan through the use of deepfakes technology. The synthesis of the two approaches helps the research to initially grasp the reach and proliferation of deepfake media in the civil society and subsequently develop the more intimate implications among the major stakeholders in the side of national security.

The research can facilitate a completely sequential explanatory design because it first offers broad patterns of relations between deepfake content and the perceptions and behaviours of the population and then presents detailed opinions of the experts about the strategic implications of nuclear deterrence. Such a design permits quantitative results to assist in the interpretation and direction of qualitative interviews so that ultimate cognizance of the research issue is acquired (Ivankova, Creswell, & Stick, 2006).

In the quantitative part, the information is taken on the most popular social networks like Twitter, Facebook, and YouTube. These websites are best suited to comprehending the extent and impact of the videos on deepfake as people and groups utilize them by sharing news, views and materials. Using data mining techniques to identify deepfake videos that appear to simulate nuclear threats or and nuclear and Pakistan related provocations uses an automated mechanism designed to conduct the collection of large quantities of information. Artificial intelligence (AI) is used to select the appropriate material according to the key terms, including the ones like Pakistan nuclear threat, deepfake, and nuclear video hoax (Chesney & Citron, 2019).

This qualitative issue of the study is going to take 40 semi-structured interviews with a great scope of experts. Among them are policymakers, military strategists, cybersecurity professionals and scholars majoring in nuclear deterrence. The aim of the interviews is to obtain a deeper complexion in the potential strategic implications of deepfakes to the nuclear deterrence of Pakistan. To provide some flexibility in the discussion of the topics and to allow the interviewee to comment on the issues in more detail, semi-structured interviews are used (Bryman, 2016).

Data analysis of the research is applied with the help of both quantitative and qualitative tools to receive full results. With quantitative information, it uses machine learning methods of sentiment analysis and NLP. These tools can handle large amounts of unstructured data, including posts to social media, and can be used to analyse the sentiment of the population of an area in regards to deepfake videos involving nuclear threats. Sentiment analysis classifies responses as positive, negative or neutral, to determine the effect on the deepfakes on the different demographics in respect to nuclear crisis or threats.

Thematic coding is used to analyse the transcripts of the interviews done in the qualitative data. This technique is used to recognize and classify themes that emerge repeatedly in the qualitative information with the aim of developing a better explanation of the opinion of the experts (Braun & Clarke, 2006). A thematic coding is especially effective in the cases of analyzing complex, subjective experiences, which are, in this case, how deepfakes can subvert the credibility of nuclear deterrence. A multitude of coders are used to make the analysis rigorous as well as reliable with disagreements being ironed out by discussion and consensus.

In this study, the ethical considerations are of utmost importance. A signed informed consent has been received by all the participants prior to the interviews where they understand the purpose of the study, the voluntary nature of the participation of the study and the ability to withdraw any time. Pseudonyms and de-identification of personal data allow concealing sensitive information,

as well as ensuring that the privacy standards are met (Resnik, 2015).
To guarantee reliability and validity of results, triangulation approach is used, which means that data collected with the help of various sources and methods can be compared and combined. This combination of closed social media analysis and interviews with experts will give the research the advantages of breadth that derive out of quantitative data on the one hand and depth that is associated with qualitative insights on the other. Triangulation makes it possible to minimize the possibility of bias and support the findings of the study (Flick, 2018).

The proposed mixed-methods tool provides a complex and balanced analytical grid to understand the numerous effects of the deepfake technology on the credibility of the nuclear deterrence of Pakistan. Considering the quantitative data, as well as the expert knowledge, the study can be assured of the thoroughness with which it analyzes how deepfakes can become influencing the perceptions of nuclear threats and the challenges it brings to national security. The methodology of the study is one that provides a rigorous analysis without compromising ethical standards and reliability that govern the collection and usage of data.

Results and Evaluation
The conclusion of the quantitative data against the social media and the qualitative data gleaned in interviews with experts gives a series of important answers to how deepfake technology can affect Pakistani nuclear deterrence. The outcomes show the problems of AI-generated disinformation and the consequences they have on a national level in terms of national security in nuclear strategy. The quantitative element of the presented study consisted of an analysis of the social media behavior around deepfake content that pertained to nuclear threats against Pakistan. To define and film the spread of deepfake videos and especially those related to nuclear problems, social media platforms Twitter, Facebook, and YouTube were employed. These videos were monitored so as to monitor them during a time of increased geopolitical tensions, where at one point there was much international attention on a possible nuclear war between India and Pakistan.

Among the most remarkable results, the significant increase in the circulation and the consumption of deepfake videos in times of higher geopolitical instability was identified. This consisted of the creation of false nuclear threats or military provocation of the Pakistan nuclear forces. These videos peaked in the frequency when there was international interest, i.e., a political crisis or a military standoff between Pakistan and India. The analysis of the social media outreach consequences showed evident relations between the dynamic increase of the political tensions on the one hand and the spreading of the deepfake video usage on the other one that means that the growing popularity of the deepfake videos is directly linked to the escalating real-life conflicts.

Sentiment Analysis:
Sentiment analysis performed on a sample of social media posts showed a more complicated picture of the reaction of people to deepfake material. Most of the posts were either dismissive or skeptical about the authenticity of the deepfake videos but a significant number of texts were confused or concerned about the truthfulness of the material. Most viewers doubted the reality of the content and some even argued that these were the actual threats or claims of the Pakistani

authorities. This confusion highlights the challenge of telling the difference between the real and the fake content and that is at the heart of the deepfake problem. Although part of the audience kept in mind that it might be manipulated, a big segment of the audience showed that they were not quite sure about the message, and it might end up having the long-term effect on the trustfulness of nuclear deterrence.

Also, part of the social media users took an active part in the discussion about the impacts of these videos which also unveiled how profound an issue deepfakes may be to evolve the discussion of nuclear threats. This kind of ambiguity may also lead to failure in facilitating communication of nuclear strategy of Pakistan because it would be difficult to believe in the message communicated by the state with other outsiders or even adversaries.

Subsequently, the qualitative component of the research consisting of 40 semi-structured interviews with a variety of security specialists, policymakers, military leaders, and cybersecurity experts offered more profound insight on the perceived threats that deepfakes elicit to the nuclear deterrence in the Pakistani context.

Depending on views, analysts disagreed on how serviceable the Pakistani nuclear position was toward deepfake threats. Others pointed out that the nuclear deterrence in Pakistan is engrained with the fact that Pakistan has long maintained its strategic beliefs, one of which involves keeping ambiguity as to the size and specific feature of its weapons of mass destruction. According to them, this ambiguity paired with the credible commitment of Pakistan to the retaliation would assist in keeping the credibility of its deterrent even despite the disinformation campaigns. These analysts also wrote that although this technology might end up causing confusion, the main tenets of Pakistan nuclear policy which is primarily its long-term image about its strategic ambiguity would remain an effective deterrence.

The respondents in the form of policymakers who participated in the study also conveyed their fears of a risk that the use of deepfakes may impair the Pakistani nuclear deterrence plan. They also emphasized the fact that Pakistans deterrence much lies in strategic ambiguity as the country has a predetermined policy of not overtly announcing the size and extent of its nuclear possessions. Such ambiguity in the threat along with the threats of nuclear retaliatory actions every now and then serves to keep adversaries at bay and prevent aggressive actions. Nevertheless, this has been balanced by creating a deepfake content that could misrepresent nuclear stance of Pakistan or even nuclear tests that might destabilize this approach. When deepfake videos seem to declare Pakistan attacking militarily or threatening some conflicts with nuclear tools, it might inadvertently oblige the nation to explain its position and consequently erode its deterrence.

Also, the leaders of policymaking indicated that with the emergence of deepfakes, Pakistan might be unable to sustain its level of trust and credibility to hold its deterrence efforts. In case of uncertainty by adversaries regarding nuclear threats or provocations being honest or fake, it may create uncertainties in the decision-making activities, or the sending/receiving of the signals at the time of acute tensions. The ambiguity that deepfakes may bring may turn out to be a hindering

factor of the main principle of nuclear deterrence, which is a clear and believable expression of will.

Although the danger presented by deepfakes to the nuclear deterrence of Pakistan is valid, there seems to be a kind of immunity even to such threats due to the accepted credibility of the nuclear strategy of Pakistan as postulated by the studies. This is because Pakistan has had decades of meticulous planning surrounding its nuclear posture, and this characteristic has been encouraged by history that has seen credible and consistent signaling, thus adding strategic stability to the region. Nonetheless, the AI-made deepfakes pose an entirely new dimension of information manipulation, and therefore Pakistan needs to respond to the challenge in order to preserve its nuclear deterrence.

The increased popularity of deepfakes demonstrates that Pakistan should improve its cybersecurity capabilities and formulate a plan to counteract AI-led lies and discredit them. It will be essential to boost the capacity of digital forensics and collaborate with international partners in order to develop norms and regulations when it comes to the application of AI in military and security affairs. As well, the study highlights the role of public and policymaker education regarding possible risks of deep fakes, and the enhanced transparency of nuclear communications as means of reducing confusion.

Discussion

Findings of this study indicate that although the application of deepfake technology presents a new and significant threat to the nuclear deterrence policy pursued by Pakistan, the credibility that the country has engendered in its nuclear policy over a very long period of time is not in much jeopardy. The nuclear deterrence of Pakistan has evolved through the decades and is backed up by its strategic doctrine of ambiguity and effective communicating messages of the risks of nuclear aggression. Although the threat of digital manipulation via deepfakes is increasing, the novelty of the strategy endorsed by Pakistan to improve its nuclear capabilities, which lies in the unambiguous threats of retaliation, is still quite sound. Nevertheless, the dark side of the new technology that involves deepfakes is the absence of protection against new types of manipulative photos and videos released on the Internet.

The results highlight the necessity of Pakistan to increase its AI and cybersecurity considerably. Since the deepfake content can very quickly change the views of people about the nuclear posture of Pakistan and generate false images around the country, it is high time that Pakistan invests in the best kind of technologies, which can counter the same. It would demand not just the cultivation of internal capabilities but the support of the close cooperation with world cybersecurity agencies and technology firms. The international character of the spread of deepfake makes it necessary that Pakistan participates in the active digital forensics and verification of information policies. With the increased technological faculties that will be able to detect and debunk deepfakes, the integrity of the deterrence messaging in Pakistan will be upheld against these forms of artificial intelligence-based disinformation campaigns.

Moreover, it is necessary to introduce generational collaboration to fight the increasing menace deepfakes in terms of nuclear weapons and international security. States should collaborate with each other to develop international norms and guidelines on how AI-generated media are created, distributed and used since, as deepfakes can be utilized to create geopolitical tensions, they can be utilized to undermine the cyber-security of another state. The United Nations (UN) and the International Atomic Energy Agency (IAEA) are examples of institutions that can be very instrumental in creating a dialogue about responsible use of AI in military at large. Creating multilateral systems of tackling deepfakes in a form of treaties or an agreement on ethical AI use would improve the international response to digital misinformation and guarantee that states can have confidence in the nuclear-armed states communications.

Although this study can get vital information, there are limitations which exist to it. The scale of information gathering is also one of the major problems, especially regarding the continually changing aspect of deep fake technology. The complexity and availability of deepfake algorithms could pose a challenging problem to the existing detection tools as more people pursue those capabilities in their search to obtain the scope of the threat. Also, the high speed of technology growth implies that the conclusions made in the course of this study do not reflect the future development of AI-generated content fully. With the appearance of new tools and methods to create and detect deepfakes, additional studies will be required to respond to such developments in order to update the methods of managing the relevant risks.

Conclusion

This paper highlights the emergence of threats that deepfake technology can pose to Pakistan with regard to its nuclear deterrence plausibility. The deepfake technology, which can produce so realistic fake messages, poses a great threat to the communication of the nuclear strategy of Pakistan. The capability to exploit the use of AI-generated media to simulate nuclear threats or military escalation actions could damage the authenticity of the nuclear stand of Pakistan, setting in confusion and ultimately arousing misunderstanding by aforesaid rivals or the international community (Chesney & Citron, 2019).

Nevertheless, Pakistan has one of the most viable nuclear deterrence strategies to date because its use of strategic ambiguity and retaliation threat credibility have been long-existing (Hussain, 2018). The credibility that the country has developed in its nuclear deterrence strategy will help it avoid the damaging effects of deepfakes in the short term. However, as the technology of AI continues its development, Pakistan needs to take a proactive approach to enhancing its security in the digital domain to withstand its strategic communications. The enhancement of cybersecurity systems, the investment into artificial intelligence-based methods of detecting deepfakes, and the cooperation with foreign allies is essential to reduce the dangers that deepfakes may have.

References

Bauer, S. (2019). Digital Warfare and Nuclear Deterrence: Bridging the Gap. Military Strategy Review, 19(2), 68-84.

Betts, R. K. (2008). Nuclear Proliferation and the International System. Strategic Studies

Quarterly, 2(3), 44-59.
Binnendijk, H. (2004). Nuclear Deterrence and Security in the 21st Century. International Security, 28(2), 52-79.
Boulton, T. (2018). Countering Disinformation: The Role of AI in Security. Journal of Digital Security, 15(2), 102-119.
Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101
Bryman, A. (2016). Social Research Methods (5th ed.). Oxford University Press.
Chesney, R., & Citron, D. K. (2019). Deepfakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107(5), 1753-1796.
Creswell, J. W., & Clark, V. L. P. (2017). Designing and Conducting Mixed Methods Research (3rd ed.). SAGE Publications.
Faris, R. (2020). The Impact of Deepfake Technology on National Security and Policy. Cybersecurity Policy Review, 14(1), 76-98.
Franks, B., Jernigan, C., & Nader, M. (2020). The Rise of Deepfakes: Implications for Geopolitics and National Security. Global Security Review, 15(1), 28-45.
Flick, U. (2018). An Introduction to Qualitative Research (6th ed.). SAGE Publications.
Gartzke, E. (2011). The Affinity of Nuclear Weapons and Security. Security Studies, 20(4), 500-533.
Glaser, C. L. (1999). The Security Dilemma Revisited. World Politics, 44(1), 3-43.
Harrison, T. (2019). Artificial Intelligence and the Future of Global Security. Global Policy Journal, 19(4), 22-35.
Hussain, S. (2018). Pakistan's Nuclear Strategy and Deterrence: Historical Context and Contemporary Relevance. Strategic Studies, 38(4), 57-79.
Ivankova, N. V., Creswell, J. W., & Stick, S. L. (2006). Using mixed-methods sequential explanatory design: From theory to practice. Field Methods, 18(1), 3-20.
Jackson, R. (2016). Cybersecurity and the Age of AI. Routledge.
Jaspal, R. (2020). Nuclear Deterrence and Digital Misinformation: How Technology Is Changing International Security. International Affairs Review, 44(3), 67-85.
Jervis, R. (1978). Perception and Misperception in International Politics. Princeton University Press.
Kalra, R. (2015). The Role of Nuclear Deterrence in South Asia: A Policy Perspective. International Politics, 52(6), 765-787.
Katz, M. (2019). The Geopolitical Consequences of Misinformation in the Digital Age. Journal of International Politics, 17(3), 201-215.
Kelley, L. (2020). Deepfakes and Nuclear Security: Navigating the Threats. Journal of International Security Studies, 16(2), 115-134.
Kello, L. (2017). The Virtual Weapon and International Order. Yale University Press.
Krepinevich, A. F. (2015). Cyber Threats and the Changing Face of Warfare. National Security Journal, 31(4), 112-127.
Lister, S. (2017). Security, Technology, and National Power: Deepfakes and Digital Security. Journal of Cybersecurity Policy, 9(2), 140-162.
Mazarr, M. J. (2018). The Korean Nuclear Crisis: U.S. Policy and the Limits of Deterrence.

Cambridge University Press.
Mistry, D. (2018). South Asian Security and the Nuclear Question. Oxford University Press.
Nye, J. S. (2004). Soft Power: The Means to Success in World Politics. PublicAffairs.
Sagan, S. D. (1996). Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb. International Security, 21(3), 54-86.
Sagan, S. D., & Waltz, K. (2017). The Spread of Nuclear Weapons: A Debate Renewed. W\. W. Norton & Company.
Schelling, T. C. (1960). The Strategy of Conflict. Harvard University Press