UDC 004.8:350

DEEPFAKES AND NATIONAL SECURITY: POLICE STRATEGIES FOR COUNTERACTION

Makalish B.[1]; Podvalnyi A.[2]; Serheiv A.[3]; Ponedilok V., Cand. Sc. (Technology), Assoc. Prof.[4]

[1,2,3,4]Kharkiv National University of Internal Affairs

[1,2,3,4]Ukraine, Kamianets-Podilskyi

[1] bohdan.makalish@gmail.com; [2] arsenyi123123123@gmail.com; [3] svp122122@gmail.com; [4] ponedilok@gmail.com

[1] https://orcid.org/0009-0002-2500-2734; [2] https://orcid.org/0009-0003-5906-130X; [3] https://orcid.org/0009-0008-7727-3687; [4] https://orcid.org/0000-0001-9669-3857.

Abstract. *During the reserch considered effects of the deepfake technology on the national security and outlines the police role in combating the dissemination of fake content. Contemporary approaches to identifying fake material, legal considerations and the necessity to enhance the digital literacy of citizens are examined.*

Keywords: *national security; deepfake; police; cyber threats; artificial intelligence.*

Introductory part. Digital media technologies are changing faster than ever, prespecified with extremely prominent position deep-fake technologies. Deep fakes are mechanisms for creating pictures, audio recordings and video footage using artificial intelligence and machine learning algorithms. These processes allow the proper reproduction of a person's appearance, voice and behavior patterns. Initially, such technologies used to gain popularity mainly in the entertainment, cinematography, and advertising industry. But in current situations, they are subjectively threatening to national security. In the current state of the tragedy of hybrid warfare in Ukraine, the country is particularly vulnerable to the spread of fake materials that have the potential to alter the consent of the people, destabilize the process of political governance, and cause crises of governmental administration.

The aim of this research is to analyze the threats posed by deep-fake technologies to national security and to determine the role of the National Police of Ukraine in countering them effectively through digital forensics, legislative regulation, and public awareness.

Main part. The danger of deepfake is multidimensional. First, they are effective tools for population manipulation through means of information manipulation. By recording speeches given by government officers, propagandists are able to distribute false information regarding politics, economics, or war, and hence create panic or mistrust among citizens. Second, deepfakes can be used to extort, violate privacy and cause reputational damage, which has not only psychological impacts but also results in political and economic impacts. Such facts create new challenges for law-enforcement organizations in general and for the National Police of Ukraine in particular, as well as the need for specialized methodology of detection and counter-measures [1].

In modern times, police forces are not just conventional outliers in ensuring safety of the public, but active players in the digital security infrastructure of the nation. The increasing use of deep-fake technology also means that it is particularly important for cyber police teams to have intelligence and analytical tools to track and report on digital threats. This includes the implementation of algorithms for the detection of counterfeit audiovisual content, the use of artificial intelligence systems for transcoding assessments, and working with platforms and organizations around the globe to make them as efficient as possible in responding swiftly to the outbreak of criminal material. Setting effective digital forensic techniques is one important factor in countering deep-fakes.

The ever improving capabilities and developments of generative neural network technologies are making detection more difficult. Thus, police departments will need a combination of tactics such as metadata mining of media files, illumination, facial geometry, and lip sync anomalies, vocal

analysis of individual voices, and behavioral analysis of people appearing in video streams. Among these techniques we read, the cooperation between subjects works in close collaboration between the police body, the cyber security specialist and institutions that are devoted to digital security [3].

The counter-deepfake approach requires a bright-line legal regulation. Many jurisdictions have already been passing laws that define allowable boundaries when it comes to deep-fake technologies, that make the creation of harmful content a crime and create, by extension, accountability systems to circulate this content. The bringing of national legislation into line with swiftly developing technological circumstances is a pressing issue in Ukraine. Specifically, the legislative framework has to specify what is considered harmful content, ways to remove harmful content as well as ways to hold offenders accountable. This effort should be made jointly by the Ministry of Internal Affairs, the cyber police, and other relevant sectors.

Another important aspect of the counter-deep-fake agenda is improvement of digital literacy through education. Deep-fake technologies are increasingly effective in situations in which citizens' skills for critical perception of media information are reduced. Awareness-raising campaigns, citizen education and media partnerships can go a long way to countering the impact of disinformation. Within this paradigm, the role of policemen evolves to incorporate beyond the protective task, with an educational role, where, among other aspects, they explain to the population the methodologies for recognizing fake audiovisual content, providing validated information sources and, in general, acting quickly in case of emerging threats [2, 5].

The international community's experiences show that deep fake countermeasures require a holistic and non-specialist approach. Already in the United States and the European Union, specialized laboratories for the screening for forged media are in place. Algorithms for automatic classification of media content are currently being created, and platforms to allow law enforcement agencies and technology companies to collaborate are starting to appear. England can learn from these precedents to focus on the threat topography in Ukraine and adapt their policy to the resources it has, thus augmenting cooperation with international technology companies with high detection algorithms, international policing mechanisms and cyber centers [1, 4].

Another source of risk emerges by using deep-fakes in political and even military damage and gaining an advantage. The spread of fake videos created in the name of statements of government officials, military and political parties can create chaos in society and lead to social unrest. Methodologically, as a result, the policing programs designed for the detection of such substances should be operationally oriented, and the problem is only solved by close cooperation among media representatives [5].

Similarly, the use of social networking sites - where fake content spreads like a wildfire - needs to be monitored. In this context, law-enforcement agencies can use early detection algorithms and automatic mechanisms for blocking dangerous content and, therefore, significantly decreasing the potential threat of massive disinformation campaigns. In addition, palliation deferred adversary architecture models are important to an efficient deep fake countermeasure.

In combination with cyber security experts, these are tools that police agencies can use to create predictive models of potential attacks based on the milieus they disseminate themselves in the digital space, analyze the behavior of users and determine which demographic groups could become vectors whose malicious content could spread. Such preventative measures consequently predispose to not only a fast reaction to present dangers but also a risk reduction probabilistic at the early developmental phase [3].

And one more reason why it is worrying is the psychological impact of deep-affects on society. Manipulation of the public sphere shapes and can mislead perceptions of events, undermine trust in public institutions, and trigger conflictive situations. Far from assuming the Chil Revisionist threat is simply unfounded, police agencies ought precisely to embrace a twofold mandate of threat hunting while at the same time committing publicly to educate about manipulation methods used, and prove to the public methods of finding the authenticity of information. This requirement is heightened most noticeably in times of political crisis or military threat when societal cohesion is a prominent element of national security.

Conclusions. Deep-fake technologies are a serious threat to national security that demands a holistic effort from law-enforcement agencies. The National Police of Ukraine should create special departments, adapt modern digital forensic solutions, involve the interchange with the appropriate foreign bodies, and increase the issue of digital literacy among citizens. It is only possible under such an integrated, transdisciplinary approach to counter the trend of disseminating fake media effectively, and ensure the stability of the information-security situation of the nation.

REFERENCES

[1] Qureshi, S.M., Saeed, A., Almotiri, S.H., Ahmad, F., Al Ghamdi, M.A. (27.05.2024). Deepfake forensics: a survey of digital forensic methods for multimodal deepfake identification on social media. *PeerJ Computer Science* 10:e2037. https://doi.org/10.7717/peerj-cs.2037

[2] Canadian Security Intelligence Service. (14.07.2025). Implications of Deepfake Technologies on National Security - Canada.ca. *Canada.ca*. URL: https://www.canada.ca/en/security-intelligence-service/corporate/publications/the-evolution-of-disinformation-a-deepfake-future/implications-of-deepfake-technologies-on-national-security.html

[3] Singh, L.H., Charanarur, P. & Chaudhary, N.K. (07.05.2025). Advancements in detecting Deepfakes: AI algorithms and future prospects − a review. *Discov Internet Things* 5, 53. https://doi.org/10.1007/s43926-025-00154-0

[4] Shields, R. (11.06.2025). Digital forensics: Tackling the deepfake dilemma. *S-RM | Your first call for corporate intelligence and cyber security*. URL: https://www.s-rminform.com/latest-thinking/digital-forensics-tackling-the-deepfake-dilemma

[5] Cherep, O., Kaliuzhna, Y., Mykhailichenko, L., Markova, S., Naumenko, Y. (22.04.2025). Formation of a strategy for countering and identifying AI technologies in the fight against disinformation under martial law. *Technology Audit and Production Reserves*, *2*(2(82), 74–79. https://doi.org/10.15587/2706-5448.2025.327157