Use of generative artificial intelligence models for image generation in information operations (InfoOps)

K. MAJ
ORCID: 0009-0001-3164-762X
krzysmaj@mon.gov.pl

Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni
Gen. Broni T. Buka 1, 05-119 Legionowo, Poland

This paper analyzes the use of generative artificial intelligence (GenAI) models for image generation in the context of information operations (InfoOps). The study adopts a qualitative approach based on literature review and case study analysis of selected examples of synthetic visual content used in disinformation campaigns. The paper examines key components of this phenomenon, including threat actors, technologies, information influence vectors, and distribution channels. An original threat model is proposed to structure the mechanisms through which synthetic images are created, disseminated, and leveraged for influence. The findings indicate that GenAI significantly enhances the scalability, speed, and effectiveness of information operations by enabling the rapid production of highly realistic visual content. The analysis also demonstrates that the impact of synthetic images depends not only on their quality but on their integration within broader communication ecosystems. The study identifies key risks, including manipulation of public opinion, erosion of trust, and increased information disorientation. The results highlight the growing importance of interdisciplinary approaches to counter disinformation, including the development of detection methods and the strengthening of critical media literacy.

Keywords: generative artificial intelligence, image generation, information operations.

DOI: 10.5604/01.3001.0055.9905

1. Introduction

The rapid development of generative artificial intelligence (GenAI) technologies has significantly transformed the way digital content is created and distributed. Generative models, including generative adversarial networks (GANs) [1] and diffusion models [2], enable the creation of realistic images from textual descriptions, significantly lowering the barrier to entry for producing advanced visual content.

At the same time, information operations (InfoOps) [3] constitute a key component of modern hybrid conflicts and activities in cyberspace. These operations involve coordinated efforts aimed at influencing the perceptions, attitudes, and behaviors of target audiences through information manipulation. In this context, visual content plays a significant role due to its strong emotional impact.

The application of generative artificial intelligence in information operations leads to the emergence of a new class of threats related to the creation of synthetic visual content, such as deepfakes. Such materials can be used for disinformation, reinforcement of propaganda narratives, and destabilization of the information environment. The scale and speed at which such content can be generated significantly exceed the capabilities of manual production.

The aim of this paper is to analyze the use of generative artificial intelligence models for image generation in the context of information operations, focusing on the threat model, threat actors, employed technologies, and distribution channels. The study also aims to systematize knowledge in this area and identify key mechanisms of influence with implications for information security.

2. Literature review and theoretical framework

2.1. Generative artificial intelligence and image generation models

Generative artificial intelligence (GenAI) encompasses machine learning methods that enable the creation of new data based on patterns learned from training datasets. In the domain of image processing, these technologies allow for the generation of realistic visual content that can

either replicate real-world scenes or depict entirely synthetic objects.

One of the fundamental approaches is generative adversarial networks (GANs), in which a generator produces images while a discriminator evaluates their authenticity. This mechanism leads to a gradual improvement in the quality of generated data and enables the modeling of complex visual structures [1].

An alternative to GANs is provided by diffusion models, which are based on a process of progressively adding noise to data and learning to reverse this process. This approach ensures greater training stability and high-quality image generation. Particularly significant are latent diffusion models, which enable efficient generation of high-resolution images at lower computational costs [2].

Contemporary image generation models most commonly operate within the text-to-image paradigm , where images are generated based on textual descriptions [4], often achieving photorealistic results. Notable examples include systems such as DALL·E, Stable Diffusion, and Midjourney. These solutions enable the rapid creation of complex visual content without requiring advanced graphic design skills.

The increasing availability and ease of use of generative models significantly lower the barrier to entry for visual content creation. From the perspective of information operations, this translates into the ability to mass-produce realistic images that can be used to influence audience perception and shape informational narratives.

2.2. Information operations as a domain for the application of visual content

Information operations (InfoOps) constitute organized activities aimed at influencing the perceptions, attitudes, and behaviors of target audiences with information as a means of influence. Today, they represent a significant component of hybrid conflicts and activities conducted in cyberspace.

In the literature, information operations are defined as the coordinated use of various communication channels to shape the information environment and control narratives [3]. One of the characteristic models is the so-called "firehose of falsehood," which involves the mass dissemination of a large volume of messages in order to create information overload and confusion [5].

Visual content plays a particularly important role in information operations, as it is characterized by a strong emotional impact and a higher susceptibility to uncritical acceptance by audiences [6]. Its effectiveness stems from rapid cognitive processing by users and its ability to reinforce narrative messaging [7].

The development of generative artificial intelligence has significantly enhanced the potential use of visual content in information operations. Generative models enable the creation of realistic images depicting events that never occurred, thereby increasing the potential for disinformation and making the verification of content authenticity more difficult [8]. As a result, information operations can be conducted at a larger scale, more rapidly, and at lower cost.

3. Research methodology

3.1. Research objective and subject

The aim of this paper is to analyze the use of generative artificial intelligence models for image generation in the context of information operations. In particular, the study focuses on identifying the ways in which synthetic visual content is used in disinformation activities and assessing its potential impact on audiences.

The subject of the research includes image generation models based on generative artificial intelligence and their applications within the information environment. The analysis also covers the mechanisms by which these technologies are utilized in information operations, including the creation, modification, and distribution of visual content.

The study adopts an analytical approach, comprising a review of the relevant literature and an examination of available examples of generative artificial intelligence applications in the context of disinformation. Emphasis is placed on identifying potential threats arising from the use of synthetic images in influence operations.

3.2. Research questions / research problems

The main research question adopted in this study is as follows:

How can generative artificial intelligence models for image generation be utilized in information operations?

To further specify the research problem, the following detailed research questions were formulated:

1. What characteristics of image generation models facilitate their use in disinformation activities?

2. What types of visual content generated by GenAI models can be used in information operations?
3. What are the main vectors for the use of synthetic images within the information environment?
4. Which distribution channels facilitate the dissemination of generated visual content?
5. What threats to information security arise from the use of generative models?

The formulated research questions constitute the basis for further analysis, particularly in the development of a threat model and the classification of the use of generative artificial intelligence in information operations.

3.3. Research methods and techniques

This study adopts a qualitative research approach focused on the analysis of selected cases involving the use of generative artificial intelligence in the information environment. The qualitative approach was selected due to the dynamic and context-dependent nature of the phenomenon, as well as the need to examine not only the visual content itself but also the circumstances of its creation, dissemination, and use.

The primary research method is case study analysis. The cases were selected purposively according to four criteria: (1) the use or suspected use of generative artificial intelligence in the creation or modification of visual content, (2) the documented dissemination of the material in an information environment, (3) the potential or demonstrated connection with misinformation, disinformation, propaganda, or manipulation, and (4) the availability of sufficient open-source material enabling verification of the case and its context.

The selected cases represent different forms of the use of synthetic visual content, including fabricated events, manipulation of public figures, and the creation of propaganda materials. This selection enables comparison of different mechanisms through which generative AI can support information operations.

Each case was analyzed according to a common analytical scheme comprising five elements: the type and characteristics of the visual content, the context and narrative associated with the material, the suspected or documented use of generative AI, the distribution channels, and the potential impact on the target audience. Where available, additional information concerning the origin, dissemination, and subsequent verification of the material was also considered.

The empirical material was collected from publicly available online sources, including social media platforms, news services, fact-checking organizations, and other open-source materials. The analysis was supplemented by a review of scientific literature concerning generative artificial intelligence, visual disinformation, information operations, and threat modeling.

The results obtained through the qualitative analysis were subsequently used to identify recurring patterns and to develop the original threat model presented in Section 4.1.

4. Analysis of the use of generative artificial intelligence models in information operations

Recent studies highlight that AI-generated content can be leveraged to enhance the scale, speed, and effectiveness of disinformation campaigns, posing substantial challenges to information integrity and trust in digital environments [9].

At the same time, research on disinformation increasingly adopts structured analytical approaches, including threat modeling frameworks that focus on identifying actors, tactics, targets, and dissemination mechanisms. Such approaches enable a systematic understanding of how influence operations are conducted and how emerging technologies, including generative AI, reshape the information threat landscape [10].

In this context, a detailed analysis of the use of generative artificial intelligence in information operations requires a structured perspective that integrates both technological capabilities and operational mechanisms. The following sections present such an approach, beginning with the development of an original threat model.

5. Threat model

Based on the literature review, research questions, and qualitative analysis of selected cases, this study proposes an original threat model illustrating the use of generative artificial intelligence in information operations (Fig. 1). The model was developed to integrate technological, operational, and informational dimensions of the phenomenon within a single analytical framework.

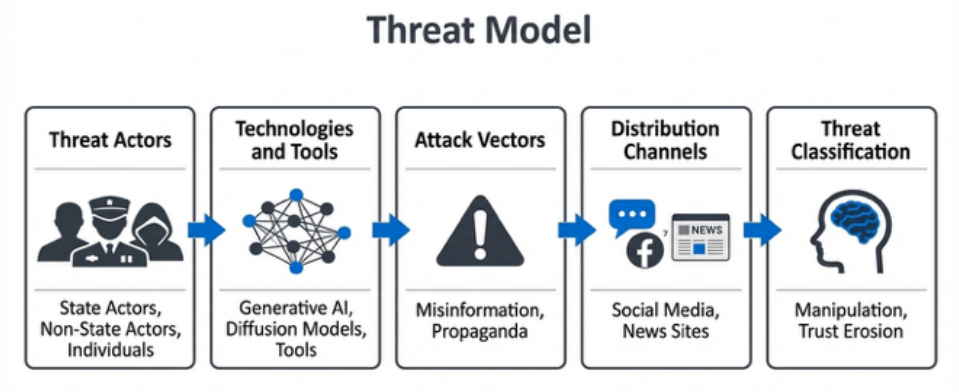


Fig. 1. Threat model of generative AI use in information operations
Source: own elaboration

The construction of the model was guided by two complementary perspectives. First, existing threat-oriented approaches to disinformation emphasize the importance of identifying threat actors, methods of operation, distribution channels, and target audiences. In particular, the framework proposed by Mirza et al. demonstrates the usefulness of a cybersecurity-inspired approach to characterizing disinformation threats[10]. Second, the analysis conducted in this study indicates that the use of generative AI introduces an additional technological layer between the actor and the resulting information effect. This layer is relevant because the characteristics and accessibility of generative tools directly influence the scale, speed, and form of synthetic content production.

On this basis, the proposed model consists of five interconnected components: Threat Actors, Technologies and Tools, Information Influence Vectors, Distribution Channels, and Threat Classification. The first component identifies the entities capable of initiating or supporting influence activities. The second describes the technological means used to generate or modify visual content. The third identifies the ways in which such content is exploited to achieve specific informational objectives. The fourth addresses the channels through which the content reaches target audiences. The final component describes the principal effects and consequences resulting from the use of synthetic visual content.

The sequential structure of the model reflects the analytical logic identified in the examined cases: an actor uses available technologies to produce or modify visual content, employs it in a specific form of influence activity, distributes the resulting material through selected communication channels, and ultimately seeks to produce an effect on the target audience or the wider information environment.

The model is therefore not intended to reproduce an existing disinformation framework, but to extend the threat-oriented perspective by introducing a dedicated technological layer and by explicitly linking the generation of synthetic visual content with its exploitation, distribution, and resulting effects. Its originality lies in applying this integrated structure specifically to generative AI-based visual content within information operations.

6. Threat actors

In the context of the use of generative artificial intelligence in information operations, the identification of actors responsible for initiating and conducting influence activities is of key importance. Threat actors differ in terms of resources, motivations, and scale of impact; however, their common denominator is the use of technology to shape the information environment.

The most advanced group consists of state actors, who employ information operations as a tool for achieving strategic and geopolitical objectives. They possess significant financial resources, access to advanced technologies, and expert support. Activities conducted by states are often long-term in nature and form part of broader influence strategies, including both disinformation campaigns and psychological operations. In the context of generative artificial intelligence, these actors may leverage advanced models to create credible visual materials supporting specific narratives.

The second group comprises non-state actors, including political organizations, ideological groups, social movements, and criminal entities. Their activities are typically more targeted, focusing on specific objectives such as influencing election outcomes, polarizing societies, or achieving economic gains. The use of generative artificial intelligence enables them

to produce engaging and easily disseminated visual content at relatively low cost, thereby increasing the effectiveness of their operations.

Individual actors also play a significant role, with their importance growing alongside the increasing accessibility of generative tools. Private individuals, influencers, and social media users can create and distribute synthetic visual content without advanced technical expertise. The motivations of this group are diverse and include ideological goals, financial incentives, and the pursuit of increased reach. The low barrier to entry means that the actions of individuals can have a disproportionately large impact on the information environment.

This typology is complemented by intermediary actors, such as social media platforms, news services, and providers of digital infrastructure. While these entities do not directly initiate information operations, they play a crucial role in their dissemination. Recommendation mechanisms, content personalization algorithms, and business models based on maximizing user engagement may contribute to the amplification of disinformation content, including materials generated by artificial intelligence.

The diversity of threat actors and their ability to leverage modern technologies make information operations increasingly complex and multidimensional. The interaction between different types of actors, as well as the blurring of their roles, further complicates the identification of disinformation sources and the effective mitigation of such threats.

7. Technologies and tools

The technological foundation is formed by generative models, particularly generative adversarial networks (GANs). However, diffusion models have recently become the dominant approach, as their process of gradually adding and removing noise ensures greater training stability and higher quality of generated images. Of particular importance are latent diffusion models, which enable efficient generation of high-resolution images with limited computational resources.

A key feature of contemporary generative systems is their operation within the text-to-image paradigm, where images are generated based on textual descriptions (prompts). This approach significantly simplifies the process of visual content creation, enabling the generation of images tailored to specific communication scenarios. In practice, this allows for the rapid production of visual materials supporting particular informational narratives.

At the implementation level, these technologies are made available through tools and platforms that eliminate the need for advanced technical expertise. Such systems offer intuitive user interfaces, real-time image generation capabilities, and functions for content modification, including changes in style, composition, and level of detail. An example of such a solution is DALL·E, which enables image generation from textual descriptions and is one of the most recognizable tools of this type.

In recent years, a clear trend has also emerged toward the integration of image generation models with large language models (LLMs). As a result, multimodal systems are being developed that enable the simultaneous generation of text and images within a single environment. This approach significantly increases the level of automation in content creation processes and allows for the coherent integration of textual narratives with corresponding visual materials.

At the same time, numerous commercial and experimental solutions have appeared on the market, often available as online services or integrated with conversational platforms. It should be noted, however, that some of these solutions lack publicly available technical documentation or detailed architectural descriptions. Consequently, in scientific analysis, they are treated as implementations of generative technologies rather than as distinct research models.

From the perspective of information operations, key characteristics of these technologies include ease of use, speed of generation, and the ability to produce realistic visual content. The integration of generative models with content distribution tools enables the creation of automated pipelines for the production and dissemination of materials, significantly increasing their potential for use in disinformation activities.

8. Information influence vectors

One of the most direct and effective information influence vectors is the creation of fabricated images depicting events that never actually occurred. Generative artificial intelligence enables the production of realistic visualizations of incidents such as attacks, disasters, or military operations, which may be perceived by audiences as authentic.

The effectiveness of such activities is particularly evident in crisis situations or rapidly evolving events, where audiences have limited ability to verify information. Under these conditions, even a single image can become a source of widely disseminated disinformation, especially if it is amplified through social media or accounts with large reach.

An example of this type of activity was the dissemination in 2023 of a synthetic image depicting a purported explosion near the Pentagon (Fig. 2). Although the image was generated using artificial intelligence tools, it was initially perceived as authentic by some users and quickly spread across social media platforms. Consequently, it led to short-term information disruption, as well as reactions in financial markets.



Fig. 2. Alleged explosion near the Pentagon
Source: https://www.itv.com/news/2023-05-23/fake-ai-created-image-of-pentagon-explosion-sparks-brief-panic

This case demonstrates that synthetic images can function as "visual evidence," reinforcing the credibility of false information. Unlike textual content, images exert a faster and stronger impact on the audience, increasing the likelihood of uncritical acceptance. As a result, generative artificial intelligence significantly enhances the potential of this information influence vector by enabling the creation of convincing visual materials with minimal effort.

Another important vector is the manipulation of the image of public figures, involving the generation or modification of images depicting well-known individuals in contexts that may influence their public perception. Generative artificial intelligence enables the creation of realistic representations of public figures without their participation, significantly increasing the risk of misuse within the information environment.

Such activities may include both portraying public figures in situations that never occurred and shaping their image in a way that deviates from reality while remaining seemingly credible. As a result, it becomes possible to reinforce specific narratives, undermine authority, or construct a false image of a given individual in the minds of audiences.

An example of such activity was the widespread dissemination in 2023 of a generated image depicting Pope Francis wearing a distinctive, stylized jacket (Fig. 3). Despite its unusual nature, the image was perceived as authentic by many users and quickly gained popularity on social media platforms.



Fig. 3. Generated image of Pope Francis in a stylized jacket
Source: https://www.nytimes.com/2023/04/08/technology/ai-photos-pope-francis.html

This case demonstrates that even content with a partially humorous character may contribute to the distortion of reality perception and increase the difficulty of distinguishing between authentic and synthetic materials.

From the perspective of information operations, the manipulation of public figures' images constitutes a particularly significant threat, as it relies on exploiting recognition and public trust. In conditions of intensive information flow, synthetic images can be easily used to influence public opinion, particularly in political or social contexts.

An important information influence vector in information operations is the creation of propaganda materials in which synthetic images

are used to reinforce specific narratives and evoke emotional responses from audiences. Generative artificial intelligence enables the creation of realistic visual scenes that may suggest public support for ideas or actions, even if such support does not exist.

An example of this type of activity was the dissemination on social media of images depicting alleged support from fans of Atlético Madrid for Palestine in the context of the Israeli–Palestinian conflict (Fig. 4). These images portrayed a stadium filled with supporters displaying symbols and colors associated with a particular political narrative. The materials were widely shared on platforms such as X and Instagram, significantly increasing their reach and impact on audiences.

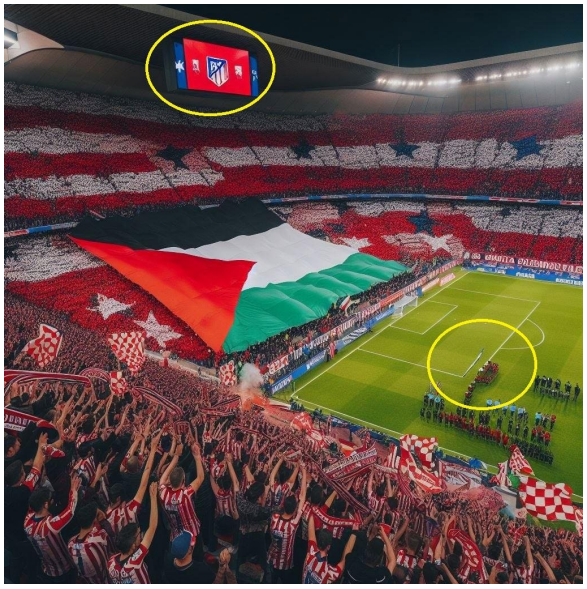


Fig. 4. Alleged support from fans of Atlético Madrid for Palestine in the context of the Israeli–Palestinian conflict
Source: https://factcheck.afp.com/doc.afp.com.33YP8AA

The image was generated using artificial intelligence tools, and the depicted situation never occurred. However, due to the high level of realism and the visual context, these materials could be perceived as authentic, particularly by individuals without the means to verify them.

This case illustrates how generative artificial intelligence can be used to create seemingly credible visual evidence supporting specific political narratives. The use of a sports-related context, which naturally generates high levels of emotional engagement, further increases the effectiveness of such messages and facilitates their wider dissemination.

From the perspective of information operations, such activities align with strategies aimed at creating the impression of broad public support for ideas. As a result, audiences may be more inclined to accept the presented narrative as widely endorsed, thereby strengthening its impact and making critical evaluation more difficult.

9. Distribution channels

Distribution channels constitute a key element of information operations, determining the reach, dynamics, and effectiveness of synthetic visual content. In the context of generative artificial intelligence, digital environments are of particular importance, as they enable rapid, scalable, and multi-channel dissemination of information.

Social media platforms play a dominant role in this domain, operating based on algorithms designed to maximize user engagement. These mechanisms favor the distribution of emotionally charged content, including synthetic images generated by artificial intelligence, regardless of their credibility. As a result, content can quickly gain popularity, significantly amplifying its impact within a short period of time.

News services and online portals also remain important distribution channels, as they may act as secondary amplifiers of information under certain conditions. Particularly in crisis situations, time pressure and the need to provide rapid updates may lead to limitations in verification processes, thereby facilitating the unintentional dissemination of disinformation.

Another category includes closed communication systems, such as messaging platforms and discussion groups, where content distribution is decentralized and difficult to monitor. In such environments, a high level of trust among participants plays a crucial role, which may lead to the uncritical acceptance of shared materials, including synthetic images.

Multimedia platforms are also significant, as they enable the integration of different forms of communication, such as images, audio, and text. Combining synthetic visual content with additional narrative elements enhances its credibility and persuasive potential, which is particularly relevant in the context of information operations aimed at cognitive and emotional influence.

From a systemic perspective, distribution channels form a complex and interconnected information ecosystem in which content can be dynamically transferred across multiple platforms. Such multi-channel dissemination leads to an amplification effect, increasing both the reach and the perceived credibility of the

message. Consequently, synthetic images generated by artificial intelligence can achieve global reach in a short period of time and produce significant social and informational impacts.

10. Threat classification

From the perspective of societal impact, the use of generative artificial intelligence in information operations leads to a range of significant systemic consequences. One of the most important among these is the manipulation of public opinion, which involves shaping the beliefs and attitudes of audiences through selectively generated and disseminated visual content. Synthetic images, due to their high perceptual credibility, can effectively reinforce specific narratives, influencing the interpretation of events and the assessment of socio-political reality.

At the same time, there is a disruption of reality perception, resulting from the difficulty in distinguishing authentic content from generated material. The introduction of a large volume of realistic yet false images into the information ecosystem blurs the boundary between fact and fiction, thereby weakening the cognitive abilities of audiences in terms of critical information analysis.

Another significant consequence is the erosion of trust in media and institutions, resulting from repeated exposure to misleading content. When audiences are repeatedly confronted with false visual materials, the credibility of information sources – including reliable ones – becomes gradually undermined. As a result, the overall level of social trust declines, negatively affecting the functioning of the information system.

Additionally, an increase in information disorientation can be observed, manifested by the overload of audiences with excessive amounts of contradictory or difficult-to-verify content. Under such conditions, individuals often abandon in-depth analysis of information, relying instead on simplified cognitive heuristics or emotional responses.

Consequently, audiences may face significant difficulties in distinguishing between true and false information, leading to a reduced capacity of society to make rational and informed decisions. This phenomenon is particularly significant in the context of democratic processes, information security, and social stability.

11. Discussion of results

The conducted analysis indicates that generative artificial intelligence significantly transforms the nature of information operations, primarily by increasing the speed, scale, and accessibility of visual content creation. Compared to traditional forms of information manipulation, image generation models enable the production of highly realistic materials at substantially lower cost and with reduced technical requirements, thereby lowering the barrier to entry for various categories of threat actors [11].

This phenomenon should be considered within the broader context of the growing importance of artificial intelligence as a component of states' strategic capabilities, including their ability to control information resources and shape the digital environment [12]. This implies that the development of generative technologies not only changes the tools used in information operations but also influences the balance of power within the information space.

The findings of this study confirm these observations, demonstrating that the availability of generative tools and their integration with digital distribution channels significantly enhance the capacity to conduct influence operations.

The results also show that the effectiveness of generative models in information operations does not stem solely from the quality of the images themselves, but from their embedding within a broader operational ecosystem. The original threat model proposed in this study effectively structures this mechanism, from threat actors, through technologies and tools, to information influence vectors, distribution channels, and final societal impacts. This sequential perspective highlights that a synthetic image alone does not constitute a complete threat, but becomes one only when combined with an appropriate narrative, distribution strategy, and reception context.

A particularly important finding is that AI-generated images can serve as a form of apparent "visual evidence," reinforcing the credibility of false information. In the analyzed cases, this applied both to fabricated events and to image manipulation involving public figures, as well as to propaganda materials. This indicates that synthetic images not only complement textual disinformation but, in many cases, become its central component, as they influence audiences more rapidly and intensely while hindering critical evaluation.

Attention should also be given to the diversity of threat actors. The study demonstrates

that the problem is not limited to state actors or organized influence campaigns. With the widespread availability of text-to-image tools and multimodal AI platforms, individual and non-state actors are also capable of conducting activities with significant disinformation potential. At the same time, intermediary actors, such as social media platforms and online portals, amplify the circulation of such content through recommendation mechanisms and engagement-driven distribution models.

The findings further confirm that distribution channels are as significant as the generative technologies themselves. Social media, messaging platforms, online portals, and multimedia platforms form an environment in which synthetic images can be rapidly transferred across channels, benefiting from amplification effects and perceived credibility. In practice, this means that the threat is not purely technological but also socio-communicative and platform-based in nature.

From the perspective of information security, particularly concerning are the systemic effects identified in this study: manipulation of public opinion, distortion of reality perception, erosion of trust in media and institutions, and increased information disorientation. This demonstrates that the use of generative models in information operations should not be viewed solely as a problem of false images, but rather as a factor weakening society's ability to distinguish truth from falsehood and to make rational decisions.

At the same time, certain limitations of the conducted analysis should be acknowledged. The study adopts a qualitative approach and is based on selected case studies and the analysis of open online sources, which means it does not cover the full spectrum of all possible applications of generative AI in information operations. Nevertheless, the presented cases are sufficiently representative to illustrate the key threat mechanisms and to justify the need for further research in this area.

12. Conclusions

The findings of this study confirm that generative artificial intelligence models for image generation constitute a significant tool supporting information operations. Their importance lies in the ability to rapidly and cost-effectively produce realistic visual content that can be used for narrative reinforcement, perception manipulation, and large-scale disinformation activities.

The study demonstrates that the use of GenAI in information operations is inherently multi-stage and can be effectively structured using the proposed threat model, which includes threat actors, technologies and tools, information influence vectors, distribution channels, and impact classification. This model provides a coherent framework for understanding how synthetic visual content is integrated into influence operations.

The analysis identifies key information influence vectors, including fabricated images of events, manipulation of public figures' images, and the creation of propaganda materials. These findings indicate that synthetic images can serve both direct and indirect influence functions, with their effectiveness strongly linked to their perceived authenticity.

The results also confirm that digital distribution channels play a critical role in amplifying the reach and impact of synthetic content. Social media platforms, online portals, messaging systems, and multimedia environments enable rapid dissemination and significantly enhance the operational potential of generative technologies.

From an information security perspective, the use of generative artificial intelligence contributes to the intensification of disinformation threats and introduces new mechanisms of influence. Addressing these challenges requires further research, particularly in the areas of synthetic content detection and the development of audience competencies in critically evaluating visual information.

13. Bibliography

[1] Goodfellow I.J., et al., "Generative Adversarial Nets", [in:] *Advances in Neural Information Processing Systems*, 27, p.1–9, Curran Associates, Inc., 2014.

[2] Rombach R., Blattmann A., Lorenz D., Esser P., Ommer B., "High-resolution image synthesis with latent diffusion models", *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition, CVPR 2022*, p. 10684–10695, IEEE, 2022, doi: 10.1109/CVPR52688.2022.01042.

[3] *NATO Military Policy on Information Operations | Public Intelligence*, public intelligence, 2012, https://publicintelligence.net/nato-io-policy/.

[4] Saharia C., et al., "Photorealistic Text-to-Image Diffusion Models with Deep Language Understanding", *arXiv*, 2022.

[5] Paul C., Matthews M., "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It", RAND Corporation, 2016.
[6] Wardle C., Derakhshan H., *INFORMATION DISORDER : Toward an interdisciplinary framework for research and policy making*. Council of Europe, 2017.
[7] Thomé de Moura R., "Risks of disinformation generated by AI and mitigation strategies", *Horizons of Multidisciplinary Studies*, Organization /ndssAurum Editora, 2025, doi: 10.63330/aurumpub.021-010.
[8] Mirza S., et al., "Tactics, Threats & Targets: Modeling Disinformation and its Mitigation", *Proceedings 2023 Network and Distributed System Security Symposium*, San Diego, CA, USA, Internet Society, 2023, doi: 10.14722/ndss.2023.23657.
[9] Malinowski M., "Cyfrowa suwerenność Polski, czyli nie tylko bezpieczne granice państwa", figshare, 2026, doi: 10.6084/m9.figshare.31802041.v1.

Wykorzystanie modeli generatywnej sztucznej inteligencji do tworzenia obrazów w operacjach informacyjnych (InfoOps)

K.MAJ

Niniejszy artykuł analizuje wykorzystanie modeli generatywnej sztucznej inteligencji (GenAI) do tworzenia obrazów w kontekście operacji informacyjnych (InfoOps). W badaniu zastosowano podejście jakościowe oparte na przeglądzie literatury oraz analizie studiów przypadków wybranych przykładów syntetycznych treści wizualnych wykorzystywanych w kampaniach dezinformacyjnych. W pracy omówiono kluczowe elementy tego zjawiska, w tym aktorów zagrożeń, technologie, wektory ataku oraz kanały dystrybucji. Zaproponowano autorski model zagrożeń, który porządkuje mechanizmy tworzenia, rozpowszechniania i wykorzystywania syntetycznych obrazów w działaniach wpływu. Wyniki wskazują, że GenAI istotnie zwiększa skalę, szybkość oraz skuteczność operacji informacyjnych poprzez umożliwienie szybkiego generowania realistycznych treści wizualnych. Analiza pokazuje również, że oddziaływanie syntetycznych obrazów zależy nie tylko od ich jakości, lecz także od ich osadzenia w szerszym ekosystemie komunikacyjnym. W pracy zidentyfikowano kluczowe zagrożenia, takie jak manipulacja opinią publiczną, erozja zaufania oraz wzrost dezorientacji informacyjnej. Uzyskane wyniki podkreślają rosnące znaczenie podejść interdyscyplinarnych w przeciwdziałaniu dezinformacji, w tym rozwoju metod detekcji treści syntetycznych oraz wzmacniania kompetencji odbiorców w zakresie krytycznej oceny przekazów wizualnych.

Słowa kluczowe: generatywna sztuczna inteligencja, generowanie obrazów, operacje informacyjne.