DEEPFAKE – MISINFORMATION, PROPAGANDA AND INFORMATION WARFARE

Wg Cdr Anand R Navaratna

Abstract

Since World War II, the ill effects and benefits of misinformation and propaganda in the face of war is well documented and, researched. By leveraging Artificial Intelligence (AI) and Military Intelligence (MI), deepfakes enable creation of hyper-realistic synthetic media, posing unique challenges to confidentiality, integrity and accessibility of military information systems. The paper explores historical examples of misinformation such as World War II, the Cold War and evaluates as to how deepfake has transformed psychological operations, deception strategies and non kinetic warfare. The paper highlights the plausible opportunity through military training, strong command structure, digital awareness and regulation of technology. The paper highlights the need to develop dual use capability viz., offensive and defensive. The challenges to adaptation of this technology is deliberated. With strong ecosystem, the military can effectively develop India specific solutions to achieve digital supremacy in joint information warfare.

INTRODUCTION

The migration from information to misinformation is historically docketed and well-researched. The reference to the use of misinformation to win a war is also an established truth from time immemorial. Misinformation spread is usually attributed to either winning through overselling the preferred narrative or psychologically rallying a popular narrative to gain popularity and fame. In the context of using propaganda for

winning a war, there cannot be a better narrative than the Second World War. If propaganda and misinformation are the ways to spread narrative, deepfakes have emerged as a popular means to undertake such propagation with the evolution of technology. This paper defines deepfake as a technology and considers a few examples as a case study. In the subsequent sections, we also analyse how deep fakes emerge as powerful 'misinformation tools'.

PROPAGANDA AND MISINFORMATION IN WORLD WAR II

The World War II provided an exemplary narrative of how print and radio were used to sell the popular narratives of the Governments of the day. A dedicated minister and a dedicated ministry of propaganda under the German Army altered the narrative of war. Further, these were used as tools to rally support for the Government, demoralise the enemy and tilt the favour in support of the German Army. If Germany used these to disseminate misinformation, the Allies used media to portray their great victories and undertake mass recruitment for their Armies. In the previous research lessons from World War II established that propaganda and misinformation can:

- **Mobilise Citizens.** Governments used radio, print, and movies to appeal emotionally and mobilise the citizens. Films like 'Why We Fight' of 1942 were used to imbibe a sense of patriotism and duty towards the nation.[1] Posters with 'I Want you' were also great for soldier recruitment (Fig 1). The Office of War Information controlled and crafted the news that did not undermine unity

Fig 1 : US Army Enlistment Poster. **Source:** USA National Achieve Catalog, https://catalog.archives.gov/id/513533

and righteousness. The main aim of this initiative was to bolster morale and encourage enlistment.[2]

- **Control of Information.** The governments held tight to unfavourable news about the war. They censored the information suitable for the Government and its war effort as it's depicted in Fig 2. The British Ministry of Information managed the press and even encouraged self-censorship amongst journalists.[3] The image of the country and soldiers' goodwill were weighed over

Fig 2 : 1945 German Propaganda Poster. **Source:** US Holocaust Memorial Museum, https://encyclopedia.ushmm.org/content/en/photo/1945-nazi-propaganda-poster

the facts and ethics on the ground. Under Joseph Goebbels, there was an effort to build the Nazi narrative surrounding Hitler, war glorification and victories of Germans.[4]

- **Enemy Bashing.** The press emerged as an effective platform to build a narrative. It was a channel to undertake enemy bashing. The barbaric acts of the enemy were graphically presented.

Further, the Nazis used media to depict Jews and other minorities as a threat to societal well-being resulting in widespread anti-semitic sentiments within the boundaries of their own country.[5]

THE COLD WAR ERA

Misinformation and propaganda contributed immensely to war efforts even after World War II, from the widespread coverage of the Nuremberg Trials to the emergence of the USSR as a potential threat to the American Dream, which received widespread coverage, building a narrative and helped to galvanise popular public sentiments. The Cuban Missile Crisis, the American Lunar mission, the USSR Sputnik mission, nuclear tests and the Warsaw-NATO narrative were a few of the instances that helped build upon the narrative aiding Information Warfare in the 'no war' scenario also. The evolution of media in terms of 'coloured print' and 'better printing technology' helped scale up the news. The population's access to news and interest in worldly affairs grew exponentially. The misinformation and propaganda surrounding the 'USA-USSR' cold war captured the imagination of a generation of citizens leading up to the disintegration of the USSR and the emergence of Russia.

POST COLD WAR ERA

The use of misinformation, propaganda and over selling of incidents did continue even after the Cold War era. The Gulf War was one such use case. A captured American solider was rescued and this incident was used to boost the morale through sensationalisation of news.[6] The color TV had emerged and it captured the imagination of people. The Kosovo War, Afghanistan invasion and search of NATO for weapons of mass destruction narrative was played in front of the world by a galaxy of news channels. The countries as per their local narrative tried to build up the event. Further with emergence of .com boom, the blogs and online news portals played their analysis, narrative and propaganda. With .com boom, the terrorists started using these sites for recruitment. ISIS and Syrian civil war saw widespread utility of these sources. In no time the Facebook and Twitter had emerged. These social sites were

used to decimate biased narrative using doctored images or videos to influence public opinion.[7] Also, Ukraine conflict saw increased use of digital platforms in spread of misinformation.[8]

In recent times, with technology, scale and reach, the missing parameter in the spread of misinformation and propaganda was 'authenticity and trust'. AI and its computing power today can establish these. Some cases exist where the computed or constructed images/ videos appear more genuine than the original content. Further, the ability to portray as an imposter has an exponential effect. Here, an imposter can digitally disguise himself or herself as a political figure, military leader or terrorist. Technology provides the ability to make the fake narrative as accurate as possible.

DEEPFAKE

Deepfake combines two words, 'deep', which is taken from a deep learning technique, and 'fake', which means non-real. It is an artificial intelligence capability built using machine learning algorithms to create synthetic media representing something or someone. The outcome can be just a voice or a video with voice. Technology has evolved so much that it becomes challenging for general citizens to discern real from fake. The misinformation created has a profound impact as it can alter public opinion, distort reality, and instil fear and unrest. Though the image, voice or video creation follows a complicated technology, the result is easy to distribute. The authenticity of deepfake aided by digital distribution like social media, WhatsApp or YouTube can escalate public sentiment in no time. The scale and time to reach a large sect of people is lightning fast. Thus, this technology can bolster misinformation and propaganda. It is an ideal weapon and catalyst in Information Warfare (IW).

DEEPFAKE TECHNOLOGY

Deepfake is built around the use of deep learning algorithms. The most popular one is Generative Adversarial Networks (GANs). The intent of this paper is not to dwell deep into the technology itself; it will be interesting to comprehend the sophistication of technology used in the

creation of synthetic data. GANs override the technology called 'neural networks'. These are called neural networks, as in function, the working is akin to human neurons. The GANs consist of two components: the generator and the discriminator. As the name suggests, the generator is responsible for generating final video audio or synthetic data.

On the other hand, discriminator extracts feature online of actual images of the person in question. This duo of generator-discriminators competes to provide better synthetic output while extracting features of authentic images or videos.[9] With time, the discriminator is trained to extract features surrounding the person of interest, while the generator is trained to generate quality data. As GANs are based on neural networks, the ability to continually learn and improve is this technology's most significant contribution and feature.

The training dataset constitutes a collection of images and videos of the target. The encoders –decoders are used to extract features through this large dataset. The encoder compresses the input data while the decoder reconstructs it. Thus, the knowledge these encoders-decoders gain can transfer facial features, expressions, and voices from one individual to another and from one context to another. Once the features are mature, the training of neural networks can be interoperable and used in different contexts or narration without much effort. Thus, this technology also improves adaptability. An individual with malicious intention can recreate the features suiting a new context using knowledge of trained data of different contexts.

FEATURES OF DEEPFAKE

In the context of IW, deep fakes bring the following features to the table:

- **Face Swapping.** In the simplest form, one's face can be superimposed onto someone else's body. The technology provides seamless integration into the body and provides facial movements and expressions, making it difficult for viewers to discern. The illusion makes viewers believe the act performed by an individual is genuine.

- **Voice Synthesis.** By training the speech of the target individual, modulation, tone, pitch, and cadence can be altered to suit the act. Thus, an individual's realistic audio or voice can be generated. The algorithms are so mature that voice can be generated for speech or text. These voice notes are widely circulated over social media to spread misinformation.
- **Text to Video.** There is ongoing work with significant progress around using text descriptions to create a video. This is possible by using natural language processing capabilities with visual generation tools. Thus, a new video can be generated quickly using textual input.

CHARACTERISTICS OF DEEPFAKE

A few of the notable characteristics of deep fake which are relevant in the context of information warfare are:

- **Credible.** The algorithm and creation of deepfake are computationally daunting but effective in quality. The synthetic image audio or video appears to be expected to the viewer. Thus, the target illusion is credible in quality.
- **Scale.** Deepfake illusion, once generated, can be circulated like a regular multimedia file or attachment for distribution. Though generation of deepfake is a professional task, there are no particular requirements to replay the file. Thus, scaling deepfakes for wider reach is easy.
- **Speed.** The generation of deepfake is aided by the quality and computational power of the computer. However, the speed at which it can spread misinformation is high. Also, this becomes a regulating challenge once a deepfake is in circulation.
- **Ubiquitous.** With increased front-end and easy-to-use software, anybody with access can create a realistic synthetic outcome. Thus, the technology is becoming increasingly ubiquitous. Also, the encoder-decoder learning can be adopted interoperable to

different context and scenario for creation of synthetic video/ image or voice.

USE CASE OF DEEPFAKE

In one of the famous applications of deepfake, US House Speaker Nancy Pelosi appeared to be slurring her words, undermining her credibility in 2019. This sparked discussion about the ethical use and regulation of deepfake to prevent misinformation and influence political discourse. In the entertainment industry, there have been instances of videos being created that featured celebrities in compromising situations. This has the potential to cause harm and emotional distress. As per a study, only 30% of respondents could accurately identify a deepfake video.[10] This advanced technology, aided by a lack of awareness, leads to the potential manipulation of public perceptions. The repercussions do not just stop here. As per a 2020 study, people exposed to deep fake videos, in general, are found to question the authenticity of all media, leading to generalised scepticism that could erode trust in legitimate news outlets.[11] Further, individuals exposed to emotionally charged deepfake content were more likely to alter their opinion on political issues.[12]

INFORMATION WARFARE APPLICATIONS OF DEEPFAKE

Technological development has a direct implication on the country's military. Arguably, misinformation and propaganda do not involve the military in general or soldiers in particular. However, the use of deepfake is not limited to the spread of misinformation and propaganda itself. The Confidentiality, Integrity and Accessiability (CIA) triad, called in the context of information security, can be potentially breached using deepfake. Once done, the sensitive information can be extracted for operational benefit and to train the deepfake models for more considerable military gains. The potential military applications of deepfake are:

- **Psychological Warfare.** Deepfake can be used to influence and affect the morale of the troops. The misinformation can be about troop deployment, pay and pensions, social fabric, family values, or political issues. These videos, images, or voice notes can be

circulated on social media or extensive messaging services, which are beyond the control of services to regulate. Also, this misleading information can be directed towards service personnel and their family members only, which can create greater panic and confusion. The well known and most recent example of this scenario was witnessed in Russia-Ukrainian war. In February 2022, a deepfake video of Ukraine President Volodymyr Zelensky was circulated, wherein it appeared that he is appealing to the Ukrainian forces to surrender to Russian military.[13] This led to mass condemnation of President within Ukraine. There were claims of Ukrainian forces also using deepfake videos of Russian President Vladimir Putin as a tool for pys-ops. The intercept reported a leaked document from Pentagon, showed that Department of Defense, USA has conducted advanced tests on offensive use of deepfakes and issued tenders for its use as part of psychological warfare in aid to special operations.[14]

Fig 3 : Deepfake video of Ukrainian President. **Source:** https://theintercept.com/2023/03/06/pentagon-socom-deepfake-propaganda/

- **Deception Operations.** The enemy can spread misinformation on aspects surrounding the professional competence of the corps and regiment. Aspects like 'territory captured', 'low serviceability', 'standard of soldiers and equipment' and 'pay and allowances' are a few deceptive messages that the enemy can directly affect the morale and reputation of the military. Also, family members can be targeted using suitable old methods of honey trapping, financial fraud and death news combined with deepfake narratives surrounding the life of military personnel in the family. Effective use of deepfake voice notes allows the military leadership's voice and commands to be replicated. Further, in operational communication, ATC commands can be replicated using deepfake technology to jam the medium of communication, thereby causing deception and confusion. In 2024, Russian media circulated deep fake videos in which a military general dealing with intelligence was shown to be admitting to Ukraine, being the one behind the Islamic terror attack in Moscow. This led to uproar in both Russia and within Ukraine. The BBC Verify reportedly undertook a detailed analysis of the video using advanced forensic technology and established

Fig 4 : Deepfake interview of Ukrainian Official. **Source:** Moscow attack: debunking the false claim, https://www.bbc.com/news/world-europe-68657383

that the video is edited using two Ukrainian TV broadcast which used to make a video.

Further, Northwestern University carried out a project, wherein a deceased terrorist (Mohammad al-Adnani) of Islamic State, was trained to say the same words as Syrian President Bashar al-Assad. The development involved two prong process, wherein the voice of trainer (Syrian President) was used to train a subject (Mohammad al-Adnani, who is dead) as part of their Terrorism Reduction with AI deepfakes (TREAD) initiative.[15] Another known case of short term and tactical deception was reported by Ukrainian Intelligence agency, wherein they reportedly intercepted a deepfake call between Prime Minister Denys Shmyhal and CEO of Turkish drone manufacturer Baykar having a conversation of cancelling drone supply orders.[16] This created considerable confusion in the minds of soldiers and drone manufacturers alike.

Fig 5 : Russian Special Services tried to use deepfake technology to contact the management of Baykar on behalf of the Prime Minister of Ukraine. A frame from the DI`s video. **Source**:https://mil.in.ua/en/news/ukrainian-intelligence-intercepted-the-russian-provocation-against-baykar-ceo-haluk-bayraktar/

- **Data Exploitation.** The data surrounding the life and operations of military personnel and their family can be recreated as audio, video and images. The data to train these models can be obtained from social media posts or other sources. These data, as per the requirement of the enemy, can be doctored to create confusion, deception, commit financial fraud or cause damage to the reputation of an individual. Doctored videos of honey trapping, disclosing service information and acts violating service norms can harm an individual's life and career. The service reputation is also affected. Thus, the existing service norms surrounding data of military personnel are at most premium and must be guarded. Simple off the shelf AI image-voice generation tools are used to spread misinformation and rake-up sentiments. A simple search of Gaza war provides AI generated images posted by individuals which are sensitive in nature.

Fig 6 : AI generated images of Gaza War. **Source:** https://petapixel.com/2023/11/07/adobe-stock-is-selling-ai-generated-images-of-the-israel-hamas-conflict/

There are projects reportedly undertaken to train deepfake modes based on the enemy commander's voice intercepts. These models are then trained to use synthetic voice as per mission tactical requirements. With gigabytes of data, creation of deepfake voice, video or image is not challenging. Political figures, military leaders, media influencers

and business houses are vulnerable. The digital foot print available is utilised for training the models on high end hardware of military grade.[17] Deliberate attempts to manipulate the training data of artificial intelligence and Machine Learning (ML) models to corrupt their behavior and elicit skewed, biased or harmful outputs cannot be ruled out. This approach is termed as 'data poisoning'.

- **No War No Peace (NWNP) Applications.** The capability of deepfake models can be interchangeably used. The models can be further trained with new data to make them mature. Deepfake can be used as an offensive and defensive application on the enemies during NWNP. During peace times, data extraction, model training, improvement in model accuracy, and individual target profiling can be undertaken. During war or hostile situations, a deepfake narrative can be used to carry out an offensive against enemy military personnel for operational benefit. Academic study have shown the ability of AI and deepfake to alter geo data. In military applications, by use of altered geo map, image or coordinates, a sense of deception and confusion can be imbibed leading to collateral damage. Live data related to transportation, logistic movement, ship movement or target information can be intercepted and manipulated to produce artificial or synthetic maps. Drone warfare is expected to bear the brunt of the technology. This technology is termed as 'deepfake geography'.[18]

- **Non-Kinetic, Non-Contact Warfare (NKNC).** This grey zone of application can be effectively used as per requirement. Deepfake, along with cyber warfare, can be used to affect enemy morale, spread confusion and induce chaos without the use of kinetic energy or without any kind of physical contact. Deepfakes, as per operational requirements, can be used to gain tactical advantage. However, the ethical usage of deepfake needs deliberation and policy backing. A case of use of deepfake image used by Russia to demonstrate, deployment of troop by USA against it was circulated to heighten tension between nations. These approaches are apt example of NKNC warfare.

- **Simulation and Training.** As the deepfakes are designed based on data and patterns, this technology can effectively train our troops and conduct simulated drills surrounding the operational, social and financial facets of our troops. This will help develop awareness and build confidence. USA, reportedly uses a Ghost Machine hardware for effective cloning of voice, video and images. These are then used on a high-end hardware to produce deepfake outcomes to train the special forces on scenarios of deception and deepfake. This provides the soldiers an edge to understand aspect of both offensive and defensive use of deepfake. Projects like Terrorism Reduction with AI Deepfakes (TREAD), are effective environment simulators to provide troops exposure and also train cyber troops for offensive operations.

REGULATION AND FRAMEWORK

Due to the breadth and potential harm to society, there has been an increase in demand for regulation of deepfake technology. Some have called for self-regulation, while most countries want to invoke dedicated regulation with a focus on deepfake. Some of the countries in which a thought process towards this has begun are:

- **United States of America.** Since the speaker of the house incident, the call for regulation and accountability of deepfake has increased. The proposed act is expected to reveal when deepfakes are used, especially in political advertising and spreading misinformation.[19] The state of California has laws against harm, defraud or deception in the context of revenge porn and election-related materials.

- **European Union.** The Digital Services Act is a larger umbrella that mandates misinformation and increases transparency in the context of the digital use of data. Also, the Union is mulling over a proposal to bring in an Artificial Intelligence Act to curb and regulate AI and its applications.[20]

- **United Kingdom.** The UK proposes a law to regulate all aspects

surrounding misinformation, privacy infringement and safety through the Online Safety Bill.[21]

- **India.** A few instances of deepfake have enabled the Government of India to consider a dedicated bill along with the Information Technology Act 2000, the Personal Data Protection Bill and Bharatiya Nyaya Samhita. The Government has set up a study committee to look into the impact of AI and emerging technology, including deepfake, and make suitable recommendations.

In the context of military applications, the challenge in regulation increases. The ability to use this technology both for offensive and defensive means needs ethical and legal backing. However, this aspect needs legal scrutiny and multi-country cooperation. The ability to have multilateral legal cooperation is the need of the hour. The application developer, user, and final distributor can be housed in different countries. Thus, culpability can be cross-border. Thus, the situation is challenging.

CHALLENGES TO DEEPFAKE ADAPTATION

- **Technology is Evolving.** Better algorithms, higher computational powers and better training data make the adaptation of this technology difficult. Micromanagement and standardised adoption cannot be easy. Determination of right algorithms and right dataset for training is a continuous and ongoing task.

- **Organisation Structure.** Deepfake forms part of NKNC scenario. This calls for all three services to bring change in doctrine. Placing this vertical under existing structure may pose a challenge. Also, as its non-contact and non-kinetic, there is no need to take physical arms, ammunition or delivery vehicle any way close to physical border; at same time NKNC may lead to sudden escalation and full-fledged conflict. Centralisation of decision and decentralisation of action may not be a full proof solution. Thus, command and control of this niche area will be challenging. Placing this aspect under a tri-services command can be studied. Incorporating, this along with EW, IW and Cyber

may be a natural choice in ethos; however, in spirit deepfake being characterised by deception - confusion - misinformation - propaganda, can be part of counter intelligence organisation too. Deepfake requires adaptation of sophisticated technology. The dual nature of deepfake application viz., offensive and defensive makes the choice at organisational level more complex, as our services have demarcated offensive and defensive elements at organisational command and control level. Thus, the choice for command and control is neither easy nor natural.

- **Skilled Deepfake Experts.** Military leadership around the world have acknowledged the need to face cyber threats and space threats. The skilled manpower required for offensive and defensive use of deepfake needs skilled human resource. Thus, nurturing a cadre within the existing cyber-space force or formation of dedicated unit needs deliberations. AI and ML at fundamental level are curated and ecosystem is built at national level. Defence forces who are focusing on AI/ ML applications in defence can consider development of strong workforce who is trained on deepfake creation and deployment. The essential aspect is to not only build AI/ ML experts but challenge is to have AI/ ML experts with operational orientation. This brings in the aspect of capability building in our training institutes. High end hardware, dataset specific to our offensive/ defensive use case and profiling of our adversary becomes key enablers.

- **Regulation v/s Development.** It is well-established research that over-regulation leads to a lack of development. Some even view regulation as an impediment to innovation. Deepfake sometimes can have beneficial effects, especially in a military context. In the domains of training and simulation, deepfakes can have great value. However, whether we should use deepfake for development is a question.

- **Judicial Issues.** Like the internet and all associated things, this technology needs multi-country participation. In the interest of personal data, security, and ethics, the judicial requirements

differ from those for spreading misinformation and propaganda. Further, each country has its laws, thus making the situation challenging and non-standard.

- **Ethical Constraints.** The offensive application of deepfake for military application may undergo ethical scrutiny.

- **Application v/s Data.** Applications with ease to make deepfake videos are available on the internet and in stores. However, for military applications, the dataset required for training of these algorithms cannot be generic. Thus as service and for effective joint fighting, there is a greater need to develop this dataset. Further, the capability to build application both to detect deepfake and to generate one has to be built. Off the shelf, applications developed by commercial entities may not in entirety support our purpose or may not be effective for military application. Thus, our services will need to have larger gestation period to build an effective war fighting capability.

- **CIA Triad Infringement.** It will be challenging for policymakers, regulators and the judiciary to protect the information security triad. Technologies like deepfake have a high potential to infringe on the triad and redefine it. Thus, the protection of data, especially operational data, becomes challenging. Capability to detect deepfake narratives built by enemy is key to ensure this. Thus training, equipment requirement, effective command and control aided by skill of service personnel will help in inhibiting such infringement. Also increasing digital literacy of service personnel and their families will ensure a strong data protection.

- **Public Awareness.** Owing to the reach of technology and its effect, it is imperative for nations to undertake public awareness campaigns. The enemy military may not target our military or our personnel directly but can release synthetic videos that have effect on citizens in general. The ability to discriminate real from fake and further knowledge to refrain from spreading such misinformation can go a long way in curbing the menace of deep

fake. This task is challenging owing to public participation and the educational level of various countries.

- **International Cooperation.** Given the global reach of this technology, multilateral cooperation in practicing best practices, sharing sound training values through joint exercises between services, with civil administration, paramilitary and other national military can ensure global cooperation. This will also help in seeking help in times of need. A digital coalition or consortium for coordination between militaries can be established. India being a professional and one of the largest militaries can contribute towards this at scale.

CONCLUSION

Deepfake technology has emerged as a potent tool with relevance in modern military with ability to redefine the dynamics of information warfare especially in domain of grey and NKNC. Its ability to manipulate perceptions, spread targeted misinformation and execute sophisticated deception presents significant operational risks to troop morale. Time is right for militaries to proactively incorporate deepfake in their doctrine. Enhanced training of personnel in deepfake detection and generation will make the IW approach more robust. Militaries through skill development, policy backing, ecosystem building and international cooperation can build a global digital consortium in with India can take the lead. Its ability to simulate realistic training scenarios and rabid deployment ability can prove to be force multiplier. At the same time the challenge of incorporating this technology at organisational level to ensure sound command and control would not be easy. The technology itself is developing with a need for India specific dataset and algorithm to keep out adversaries. Thus, to maintain a strategic edge, the advantages of deepfake must be adopted to supplement national defence objectives while mitigating its risks in evolving digital battle field.

★★★

Wg Cdr Anand R Navaratna is serving as Aeronautical Engineer in IAF. He has done his M Tech in Artificial Intelligence and is perusing his PhD in Digital Transformation from IIT Jodhpur.

NOTES

[1] *Jowett, Garth S., and Victoria O'Donnell. 2018. "Propaganda and Persuasion". Thousand Oaks: SAGE Publications.*

[2] *Browne, Patrick. 2020. "The United States and World War II: A History". New York: Oxford University Press.*

[3] *Harris, Sam. 2018. "Propaganda and the Public Sphere in World War II". Chicago: University of Chicago Press.*

[4] *Welch, David. 2019. "Nazi Propaganda and the Second World War". London: Bloomsbury.*

[5] *Beller, Steven. 2019. "Anti-Semitism in Nazi Germany". London: Routledge.*

[6] *Lindsey, Brian. 2015. "Media and War: The Jessica Lynch Incident." "Media, War & Conflict" 8 (3): 264-278.*

[7] *Cohen, David. 2021. "Understanding the Threat of Deepfakes." "Media Studies Journal" 15 (2): 88-102.*

[8] *Mitchell, John. 2022. "Digital Warfare and Information Manipulation: The Ukraine Conflict." "International Journal of Digital Media" 18 (4): 125-142.*

[9] *Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Courville, A. (2014). "Generative adversarial nets." "Advances in Neural Information Processing Systems", 27.*

[10] *Cohen, Adam. 2020. "The Role of Social Media in the Syrian Civil War." "Journal of Conflict Studies" 10 (1): 45-67.*

[11] *Jane Wakefield, (2022), "Deepfake Presidents used in Russia-Ukraine War", BBC News, URL: https://www.bbc.com/news/technology-60780142*

[12] *Sam Biddle, (2023), "US Special Forces want to use deepfake for Psy Ops", The Intercept, URL: https://theintercept.com/2023/03/06/pentagon-socom-deepfake-propaganda/*

[13] *Daniel L. Byman, (2023), "Deepfakes and International conflict, Brookings Foreign Policy", Brookings, URL: https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf*

[14] *Militarnyi, (2022), "Ukrainian intelligence intercepted the Russian provocation against Baykar CEO Haluk Bayraktar", URL: https://mil.in.ua/en/news/ukrainian-intelligence-intercepted-the-russian-provocation-against-baykar-ceo-haluk-bayraktar/*

[15] *Sam Skove, (2024), " How Army special operators use deepfakes and drones to train for information warfare", Defence One, URL: https://www.defenseone.com/technology/2024/04/how-army-special-operators-use-deepfakes-and-drones-train-information-warfare/395852/*

[16] *Zhao, B., Zhang, S., Xu, C., Sun, Y., & Deng, C. (2021). Deep fake geography? When geospatial data encounter Artificial Intelligence. Cartography and Geographic Information Science, 48(4), 338–352. https://doi.org/10.1080/15230406.2021.1910075*

[17] *Chesney, Robert, and Danielle Keats Citron. 2019. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." "California Law Review" 107 (5): 1753-1820.*

[18] *Mitchell, John. 2022. "Digital Warfare and Information Manipulation: The Ukraine Conflict." "International Journal of Digital Media" 18 (4): 125-142.*

[19] *HR 5586,(2023), "USA Congress", URL: https://www.congress.gov/bill/118th-congress/house-bill/5586/text*

[20] *European Parliament (2023), EU AI Act: first regulation on artificial intelligence, URL: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence*

[21] *Ministry of Justice and Laura Farris, (2024), "Government cracks down on 'deepfakes' creation", Government of UK, URL: https://www.gov.uk/government/news/government-cracks-down-on-deepfakes-creation*