

# UA: UKRAINE ANALYTICA

Issue 3 (35), 2024

INDIA POLICY  
ASPIRATIONS  
EUROPE  
INFORMATION  
RUSSIA  
DECEPTION  
CHALLENGES  
NATO  
GEOPOLITICAL  
FUTURE  
ADVANCEMENT  
TECHNOLOGIES  
ARTIFICIAL  
UKRAINE  
HISTORY  
PARTNERS  
CHINA  
ALLIANCES  
NARRATIVE  
WAR  
DEEPFAKES

- NEW WARFARE
- NATO ASPIRATIONS
- FUTURE FOREIGN POLICY



## FUTURE

### Editors

Dr. Hanna Shelest  
Dr. Mykola Kapitonenko

### Publisher:

Published by NGO «Promotion of Intercultural Cooperation» (Ukraine),  
Centre of International Studies (Ukraine), with the financial support of the  
Representation of the Friedrich-Ebert-Stiftung in Ukraine

**UA: Ukraine Analytica** is the first Ukrainian analytical journal in English  
on International Relations, Politics and Economics. The journal is aimed  
at experts, diplomats, academics, students interested in the international  
relations and Ukraine in particular.

### Contacts:

website: <http://ukraine-analytica.org/>  
e-mail: [Ukraine\\_analytica@ukr.net](mailto:Ukraine_analytica@ukr.net)  
Facebook: <https://www.facebook.com/ukraineanalytica>  
Twitter: [https://twitter.com/UA\\_Analytica](https://twitter.com/UA_Analytica)

The views and opinions expressed in the articles are those of the authors  
and do not necessarily reflect the position of UA: Ukraine Analytica,  
its editors, Board of Advisors or donors.

ISSN 2518-7481

500 copies

# TABLE OF CONTENTS

<b>THE NEW FACE OF DECEPTION: AI'S ROLE IN THE KREMLIN'S INFORMATION WARFARE</b> .....	<b>3</b>
<i>Volodymyr Solovian and Matt Wickham</i>	
<b>PERFECT STORM FOR UKRAINIAN FOREIGN STRATEGY</b> .....	<b>13</b>
<i>Maryna Karlevits</i>	
<b>NODAL DEFENCE AND UKRAINE'S NATO ASPIRATIONS.</b> .....	<b>20</b>
<i>Alexander Lanoszka</i>	
<b>RISE OF THE NEW 'AXIS OF EVIL' AND NATO'S CHALLENGING PATH AHEAD.</b> .....	<b>28</b>
<i>Yasin Yildirim</i>	
<b>THE 2024 UNITED STATES ELECTIONS AND THE FUTURE OF THE LIBERAL INTERNATIONAL ORDER</b> .....	<b>37</b>
<i>Brendan H. Gallagher</i>	
<b>CIVILIZATIONAL NARRATIVE IN THE FOREIGN POLICY OF INDIA AND CHINA: THE IMPACT OF THE RUSSIAN-UKRAINIAN WAR</b> .....	<b>48</b>
<i>Sofia Lysko</i>	

# THE NEW FACE OF DECEPTION: AI'S ROLE IN THE KREMLIN'S INFORMATION WARFARE

Dr Volodymyr Solovian,

Matt Wickham

Hybrid Warfare Analytical Group, UCMC

*The rapid evolution of artificial intelligence (AI) has empowered new dimensions of global information warfare. AI-driven technologies, such as deepfakes and sophisticated bot networks, have become pivotal tools of disinformation campaigns carried out by authoritarian regimes. This article highlights the information security threats posed by AI-driven technologies. The authors examine Russia's approach to using AI in information warfare, citing examples from the ongoing Russia-Ukraine war. The article describes Russia's attempts to prioritise AI development so as to enhance its disinformation arsenal. Also, the article emphasises the need for strong measures to counter AI misuse while adhering to democratic standards.*

In recent years, artificial intelligence (AI) has made rapid advancements. Since the advent of the 2020s, we have entered an era marked by the widespread adoption of generative AI models, capable of producing diverse forms of data. The consistent growth in the market capitalisation of companies driving AI technology advancements reflects optimism about the industry's future. Notably, Nvidia, a leading producer of computing accelerators, ranks at the top of the world's most valuable companies, followed by Microsoft (a partner of large-scale language model developer OpenAI) and Apple, which recently launched its own AI platform, Apple Intelligence<sup>1</sup>.

However, the potential threat of malicious AI being used to manipulate public perception has been a longstanding concern, and this issue is now becoming a reality.

Advances in machine learning have led to increasingly sophisticated disinformation campaigns that leverage AI. As software becomes more user-friendly and technology costs decrease, the use of AI in the disinformation sector is growing more widespread.

Today, researchers typically identify several key areas where AI is used for propaganda purposes:

- *Fake news through realistically fabricated video and audio:* For instance, videos that convincingly depict state leaders making provocative statements they never actually made.
- *Highly targeted disinformation campaigns:* Social media and messaging app users receive personalised messages designed to influence their behaviour;

---

1 Daniel Van Boom, *Apple, Nvidia, Microsoft and the race to US\$4 trillion*, 19.06.2024 [<https://bit.ly/3P9ToOD>]

a tactic often employed during election campaigns.

- *Automation of influencer campaigns:* AI-powered social media analysis identifies users who may be vulnerable to manipulative content.
- *Flooding information channels:* Large-scale information attacks use bots to overwhelm channels with noise (false or distracting information), making it difficult to access genuine data.
- *Controlling information accessibility:* AI algorithms moderate media platforms, guiding users towards specific content, while avoiding messages deemed inimical<sup>2</sup>.


In this landscape, media users and social media participants must increasingly identify high-quality forgeries generated by artificial intelligence. This undermines trust in traditional information ecosystems, fragments the information landscape, and ultimately polarises social, political, and cultural discourse.

## AI in the Global Context of Information Warfare

In recent years, AI has become an integral part of information-psychological influence campaigns on a global level. For instance, NATO's updated Artificial Intelligence Strategy emphasises the risks involved: «AI-enabled information operations might affect the outcome of elections, sow division and confusion across the Alliance, demobilise and demoralise societies and militaries in times of conflict, and erode trust in institutions critical to the Alliance.»<sup>3</sup>

This issue has become an important aspect of public debate among politicians, business leaders, and the media, as a result of numerous 'global summits' on AI security. It is indicative that in the keynote speech at the Global Media Forum in Bonn (June 2024), German Foreign Minister Annalena Baerbock remarked, «Artificial intelligence makes disinformation cheaper, easier, and more effective.»<sup>4</sup>

---

 ***the potential threat of malicious AI being used to manipulate public perception has been a longstanding concern, and this issue is now becoming a reality***

---

A pressing challenge today is the deployment of AI by autocracies, their affiliated groups, and terrorist organisations, to destabilise democracies in Western countries. The capabilities of artificial intelligence are attracting the attention of Chinese, Russian, and Iranian intelligence agencies and government units focused on external disinformation. These regimes seek to leverage AI, in order to analyse public sentiment and identify key issues fuelling public dissatisfaction.

It is worth noting that in the realm of information warfare, AI is a 'double-edged' sword, in that it can be used by both sides in a conflict. For example, Ukraine actively employs deepfake technology, mirroring Russian tactics. In some cases, the use of AI technology is part of the informational

---

2 M. Brundage, S. Avin, J. Clark, H. Toner, and others., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, Feb.2018, p.7.

3 Summary of NATO's revised Artificial Intelligence (AI) Strategy, 10.07.2024, [[https://www.nato.int/cps/en/natohq/official\\_texts\\_227237.htm](https://www.nato.int/cps/en/natohq/official_texts_227237.htm)]

4 'Democracy didn't fall from the sky,' says Baerbock in Bonn, 17.06.2024, [<https://bit.ly/3DsPmy9>]


support for conventional operations of the Armed Forces of Ukraine. During the first month of the Kursk offensive, Ukraine utilised around 30 deepfakes. Most of them targeted residents of the Kursk region as, say, in a fake video address, the governor 'calls on' men over the age of 18 to come to the military recruitment offices and receive weapons<sup>5</sup>. Such manipulations have allowed Ukraine to intensify a sense of panic among the local population and disrupt the organisation of the Russian army's defences. Ukraine also has a track record of deepfake attacks on a nationwide scale in Russia. For example, in the summer of 2023, a hacked broadcast on Russian state TV aired a deepfake Putin speech announcing a new wave of mobilisation<sup>6</sup>.

Given the global threat posed by disinformation campaigns, it is crucial to address the risks associated with one of the most rapidly advancing AI technologies – deepfakes. Synthetic video content has become an integral feature of contemporary digital ecosystems. However, unlike in Western cultures, where deepfakes are mainly used in the entertainment industry or as tools for political campaigns, they have become powerful instruments of hybrid warfare for autocratic regimes.

In non-conflict scenarios, deepfakes are frequently employed by malign external actors, particularly during electoral processes. For instance, during Taiwan's

presidential elections in January 2024, the pro-China media disseminated a fabricated video targeting LAI Ching-te, the Democratic Progressive Party's candidate, whose prospective victory was perceived as unfavourable by Beijing<sup>7</sup>. Such content is typically disseminated through networks of state-aligned media outlets and influencer bloggers, with the original sources deliberately concealed.

---



***A pressing challenge today is the deployment of AI by autocracies, their affiliated groups, and terrorist organisations, to destabilise democracies in Western countries***

---

In democratic environments, the proliferation of AI-generated disinformation by domestic political actors can obscure the infiltration efforts of external state and non-state entities, including China, Russia, and Iran. For example, in the lead-up to the U.S. elections, OpenAI reportedly rejected 250,000 requests to generate deepfakes related to electoral issues<sup>8</sup>.

The increasing prevalence of AI underscores the necessity for democracies to adopt robust mechanisms for identifying, filtering, and labelling synthetic content. These measures

---

5 Власти предупредили о фейковом видео с губернатором Курской области Смирновым (The authorities warned about a fake video with the governor of the Kursk region Smirnov), 07.08.2024, [https://www.kommersant.ru/doc/6878959]

6 «Обращение» Путина о мобилизации и военном положении оказалось дипфейком (Putin's «address» on mobilization and martial law turned out to be a deepfake), 5.03.2023, [https://lenta.ru/news/2023/06/05/fake\_radio/]

7 A. Khimiak, *Taiwan: How an Island Democracy Resists the Propaganda Onslaught of Beijing and Moscow*, Hybrid Warfare Analytical Group. 26.01.2024. [https://uacrisis.org/en/taiwan-how-an-island-democracy-resists-the-propaganda-onslaught-of-beijing-and-moscow]

8 *ChatGPT blocked 250,000 AI image requests of US election candidates*, Euronews. 11.11.2024, [https://www.euronews.com/next/2024/11/11/chatgpt-blocked-250000-ai-image-requests-of-us-election-candidates]

are essential to safeguarding electoral integrity and mitigating the risks posed by AI-enabled disinformation campaigns.

Moreover, malicious international actors may exploit AI to implant distorted interpretations and false narratives into the public consciousness. The creation of synthetic videos, images, texts, or audio can be weaponised to influence public opinion, particularly through social media. This facilitates the justification of wars and coups, for instance, as well as the falsification of orders from military or political leaders. A significant concern is that AI could potentially fabricate a 'synthetic casus belli,' offering a pretext for external military aggression.



---

***In democratic environments, the proliferation of AI-generated disinformation by domestic political actors can obscure the infiltration efforts of external state and non-state entities, including China, Russia, and Iran***

---

Additionally, advances in speech synthesis systems that can imitate the voices of specific individuals present new challenges for curbing the spread of misinformation. This technology, combined with AI's ability to adapt to local language practices, makes it increasingly difficult to detect and debunk such misinformation.

## **Deepfake as a Weapon of Russian Aggression**

Concerns regarding the deployment of AI to covertly influence the societal dynamics of adversaries have intensified, particularly as the technology has advanced into the domains of hybrid warfare since 2022. The authors of this article seek to critically examine the challenges posed by AI-driven propaganda, with a specific focus on the use of deepfakes by Russia to undermine the current Ukrainian leadership.

The first known use of a deepfake as a psychological weapon tied to Russia's full-scale invasion emerged on March 18, 2022. One version of the 'deepfake' was viewed more than 120,000 times on X<sup>9</sup>. A hacked Ukrainian news site, Ukraine24, aired an AI-generated video of President Zelenskyy, allegedly calling for the surrender of Ukrainian troops to Russian forces. In the video, the fake Zelenskyy warns, «*It is only going to get worse, much worse. There will no longer be a tomorrow. I ask you to lay down your arms and return to your families*» – a message suspiciously similar to Putin's then recent appeal to Ukrainian soldiers to surrender and accept Russian control. Ukraine24 quickly confirmed the message was a hack, while Zelenskyy reassured the nation further with a real Instagram post filmed outside the Office of the President building<sup>10</sup>.

Over a year later, in November 2023, a sharper, more advanced AI-generated video surfaced – this time featuring Valerii Zaluzhnyi, then Commander-in-

---

9 *Deepfake Zelenskyy surrender video is the 'first intentionally used' in Ukraine war*, Euronews. 16.03.2022, [<https://bit.ly/4firmvaZ>]

10 *Debunking a deepfake video of Zelensky telling Ukrainians to surrender*, France24. 18.03.2022, [<https://bit.ly/3DtbQ2ad>]



Chief of Ukraine's Armed Forces, allegedly announcing a 'coup d'état' following his supposed 'resignation.' Anonymous Russian Telegram channels and the usual Kremlin-aligned sources were quick to share the video, presenting it as undisputed 'evidence' of a spat between Zaluzhnyi and Zelenskyy. The aim was to portray Zelenskyy as an internal threat, unfit to lead, a narrative which leaned on weeks of rumours of a 'Zaluzhnyi-Zelenskyy conflict.' This, therefore, if taken at a pure content level, made the video appear plausible. And, unlike the earlier Zelenskyy deepfake, this one was refined enough that casual news followers would struggle to see through it<sup>11</sup>.

While the video had flaws – badly cut transitions and lip-syncing errors – many viewers, particularly those less familiar with the technology, would likely miss these signs. In an oversaturated information space, few people have the time or inclination to examine videos frame-by-frame, especially when the content seems to confirm their biases or fears. Moreover, the leap in quality between the Zelenskyy and Zaluzhnyi deepfakes in just a year signals a real investment by the Kremlin in weaponising AI as a psychological tool, escalating disinformation to a new level. The growing scepticism towards online content's legitimacy, driven by increasingly sophisticated AI manipulation, could lead to a broader mistrust, undermining the Ukrainian government's efforts to counter genuine threats.

These incidents served as warnings of the dangers AI would pose to Ukraine's

fight against Russian disinformation and hybrid warfare techniques, with many experts suggesting it could be just the 'tip of the iceberg' in the information warfare landscape. Hany Farid, a digital media forensics expert at UC Berkeley, and Sam Gregory from the human rights group Witness, caution that deepfakes like these «pollute the information ecosystem,» sowing a shadow of doubt throughout the media amid the 'fog of war.'<sup>12</sup>

### Russia's Sovereign AI: Empowering Propaganda

By integrating AI into its arsenal of information warfare tools, the Kremlin frequently expresses concerns about the potential use of symmetrical approaches against Russia. Publications from Russian think tanks and academic institutions often highlight apprehensions regarding the use of AI to «destabilise internal political processes» with the goal of regime change. A notable example can be found in analyses by experts from the Centre for International Information Security and Scientific-Technological Policy at the Moscow State Institute of International Relations (MGIMO), run by Russia's Ministry of Foreign Affairs. These analyses identify several objectives of Western AI applications against Russia, including: 1) altering cognitive processes within public consciousness; 2) fostering biases or reflexive thinking; and 3) exerting a negative influence on decision-making processes at both individual and collective levels. The authors conclude that «the objective is to sow discord in Russia and China, provoke conflicting narratives, polarise opinions, and radicalise groups.»<sup>13</sup>

11 *Fake: Ukrainian Commander-in-Chief Zaluzhnyi Is Preparing a Military Coup*, StopFake. 8.11.2023, [<https://www.stopfake.org/en/fake-ukrainian-commander-in-chief-zaluzhnyi-is-preparing-a-military-coup/>]

12 *Zelenskyy deepfake crude, but still might be a harbinger of dangers ahead*. Suzanne Smalley, Cybercoop. 18.03.2022, [<https://cyberscoop.com/zelenskyy-deepfake-troubles-experts/>]

13 Evgeny Pashentsev, *Report. Experts on the Malicious Use of Artificial Intelligence and Challenges to International Psychological Security*, International Center for Social and Political Studies and Consulting. Moscow: LLC «SAM Polygraphist». 2022.

In response, the Kremlin has prioritised the development of an autonomous AI ecosystem, described by President Putin during the recent ValDAI Club meeting as 'sovereign AI.'<sup>14</sup> Russian authorities believe this approach will mitigate the risk of Russian internet user data being accessed by Western intelligence agencies. Russia has initiated the development of neural networks comparable to ChatGPT. For instance, 'GigaChat,' funded by Sberbank, and Yandex's language model, 'YandexGPT,' unveiled in May 2023, represent significant advancements in this area. Yandex has since introduced an updated version, YandexGPT-4, demonstrating the model's ongoing development and refinement<sup>15</sup>.

Despite the significant financial burden of the war against Ukraine, the Kremlin plans to allocate approximately 7.7 billion roubles between 2025 and 2027 to support research centres specialising in AI. Concurrently, the federal project 'Artificial Intelligence,' which facilitates over 100 AI training programmes at Russian universities, is set to receive 25.8 billion roubles over the same period<sup>16</sup>.

Russia is also expanding its centralised institutional framework for AI development. At the federal level, the National Centre for Artificial Intelligence Development under the Government of the Russian Federation oversees the integration of AI technologies across various sectors, including the economy, research institutions, business, and the public sector. The implementation of AI in the military domain is managed by a specialised department within the Russian

Ministry of Defence, established in the summer of 2022.

In the realm of propaganda, RT (Russia Today) serves as the flagship platform for Kremlin-backed international information campaigns. Operating in close collaboration with Russian intelligence agencies, RT's efforts are bolstered by AI-driven bot farms. These bot farms amplify propaganda by generating and disseminating content at scale. The extent of this issue is detailed in a joint statement by the Federal Bureau of Investigation (FBI), the Cyber National Mission Force (CNMF), and specialised agencies from the Netherlands and Canada: «Affiliates of RT, a Russian state-sponsored media organisation, used Meliorator – a covert artificial intelligence enhanced software package – to create fictitious online personas, representing a number of nationalities, to post content on X (formerly Twitter). Using this tool, RT affiliates disseminated disinformation to and about a number of countries, including the United States, Poland, Germany, the Netherlands, Spain, Ukraine, and Israel» (July 9, 2024)<sup>17</sup>.

RT remains under constant surveillance by Western intelligence agencies. It is important to note, however, that the versatility of AI tools enables Russian propagandists to significantly expand the pool of operators disseminating pro-Russian fake content, without relying directly on RT. In practice, AI may soon autonomously manage bot networks, circumventing efforts to detect and counteract disinformation.

---

14 Путин призвал развивать в России суверенный искусственный интеллект (*Putin calls for development of sovereign artificial intelligence in Russia*), Finam. 07.11.24, [<https://bit.ly/406gnAj>]

15 V. Reed, *YandexGPT vs ChatGPT: Battle of Multilingual Language Models*, AICompetence. 28.08.2024, [<https://aicompetence.org/yandexgpt-vs-chatgpt/>]

16 Проект федерального бюджета на 2025–2027 годы принят во втором чтении, (*The draft federal budget for 2025–2027 was adopted in the second reading*), State Duma of the Russian Federation. 14.11.2024, [<http://duma.gov.ru/news/60359/>]

17 *State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity*, The Internet Crime Complaint Center. 9.07.2024, [<https://www.ic3.gov/CSA/2024/240709.pdf>]

## The Evolving Role of AI in Russian Disinformation Campaigns


Russian bot farms have long been central to the Kremlin's disinformation efforts, playing a crucial role in their strategy to influence foreign elections, destabilise nations, and advance imperial ambitions. With the rise of AI, these bot networks have evolved, giving the Kremlin, or any hostile actor, an unprecedented advantage in waging disinformation campaigns through written formats on social media.

Recent evidence of enhanced capacity has emerged on social media, where users with hacker expertise have exploited AI vulnerabilities to interrupt and manipulate bots for spreading Russian propaganda. This technique, known as 'prompt injection,' involves manipulating AI responses by bypassing the original developer instructions. It has become a key tool in the fight against disinformation, but it also poses a significant concern for AI security.

The vulnerability was first exploited when social media users, particularly on X, began to question whether they were engaging with bots. By injecting commands like «*ignore all previous instructions*,» they could disrupt the bot's trajectory, breaking its original programming and steering it towards unintended prompts from those created by the original user<sup>18</sup>. Researchers first identified this exploitation in September 2022, two months before ChatGPT's official release. By 2023, prompt injections had gone viral, with users sharing videos

demonstrating how to 'break' AI models. This quickly led to AI-powered bots being weaponised to spread disinformation. Russian-aligned narratives began to dominate the digital space, especially in places such as X, where algorithms seemed to favour Kremlin narratives, echoing tactics used during the 2016 U.S. elections but now on a much more advanced scale. A study by NewsGuard examined ten leading AI chatbots and found that 32% of the time, AI chat bots spread Russian propaganda, citing fake news sources, as credible information<sup>19</sup>.

---



***Despite the significant financial burden of the war against Ukraine, the Kremlin plans to allocate approximately 7.7 billion roubles between 2025 and 2027 to support research centres specialising in AI***

---

OpenAI has taken steps to address this issue. On July 19, 2024, they introduced a new safety feature called 'instruction hierarchy', designed to prioritise the developer's original system instructions over user-injected commands. This update is aimed at reducing the risk of prompt injections bypassing the bot's safeguards<sup>20</sup>.

While this newly-fixed flaw marks progress in securing AI models, it fails to tackle the root cause of the ability to disseminate disinformation. Russian bots continue their

---

18 J. Shane, *Ignore all previous instructions*, AI Weirdness. 23.09.2022, [<https://www.aiweirdness.com/ignore-all-previous-instructions/>]

19 McKenzie Sadeghi, *Top 10 Generative AI Models Mimic Russian Disinformation*, NewsGuard. 18.06.2024, [<https://www.newsguardtech.com/special-reports/generative-ai-models-mimic-russian-disinformation-cite-fake-news/>]

20 E. Wallace, K. Xiao, R. Leike and others, *The Instruction Hierarchy: Training LLMs to Prioritize Privileged Instructions*, Cornell University. 19.04.2024 [<https://arxiv.org/abs/2404.13208>]

relentless spread of harmful narratives, and the inability of security services to intervene in AI prompts used by these bots has only made mitigating their reach more challenging. With the battle against this vulnerability, calling out these bots – and the Kremlin’s disinformation machine – has become not just more time-consuming but less engaging for audiences. Exposing AI-prompted bots and turning their agendas into online clownery – such as ordering them to perform ridiculous injected prompts – was an effective way to counter disinformation. It exposed the Kremlin’s tactics, while offering a ‘laugh in the face’ of Russian propaganda’s attempts to distort messages in the West.



---

***As deepfakes and other AI-driven forgeries become increasingly accessible, even the most credible information runs the risk of being dismissed as fake***

---

These interventions served as a form of humiliation, showing that sometimes the best way to counter disinformation is through humour and ridicule, drawing the attention of those who might otherwise remain blind to disinformation and thus creating a safer online space. The fundamental issue, however, remains: the development of AI-driven disinformation is evolving faster than the tools designed to combat it, making it harder to trace, contain, and neutralise. This fix in AI coding essentially gives hostile actors – determined to manipulate narratives – free rein, rendering them unchallenged.

### **Ethical Dilemma for Democracies**

As deepfakes and other AI-driven forgeries become increasingly accessible, even the most credible information runs the risk

of being dismissed as fake. Despite this growing threat, democracies have been slow to adopt clear policies to address it. Their lengthy decision-making processes often allow the enemy time to shift tactics, leaving responses outdated before they can take effect. To counter the speed at which authoritarian actors leverage AI-powered disinformation, democracies must adapt quickly, perhaps employing AI tools such as deepfakes themselves – under the umbrella of strict policies that uphold democratic values. Avoiding such tools entirely out of fear of ethical concerns could leave democracies ill-equipped to counter the rapid and flexible strategies of authoritarian actors.

That said, when used responsibly, deepfakes and AI technologies have proven their potential for good. In the early stages of the war, Ukraine leveraged this technology to convey the devastating reality it was facing, by creating AI-generated videos depicting cities in Europe coming under surprise missile attack. This emotional appeal, though using AI, was aimed at pushing Europe to recognise what was at stake – «this could be your future if Ukraine fails.» The authenticity of the AI video, while still visibly artificial, was realistic enough to rally support. The video’s success was part of Ukraine’s broader foreign outreach strategy, demonstrating that AI, when used in line with democratic principles post-2022, can serve as a necessary tool for democracies. The question we are faced with now is whether deepfakes, which blur the line between reality and fabrication to an unprecedented degree, can coexist with the ethical standards that democracies claim to uphold.

Ukraine’s use of AI-generated videos, such as their depictions of an attack on the Kremlin or humorous portrayals of figures like Putin turning into putty when squeezed, highlights how AI and deepfakes can serve as morale boosters. These creations target

the source of aggression, offering a sense of ridicule and the possibility of further creative work that unifies and inspires. This approach stands in contrast to the Kremlin's weaponisation of deepfakes to spread disinformation, manipulate public perception, and erode trust.

These examples demonstrate that AI and deepfakes, while often viewed through a negative lens, can be used constructively to align with democratic values. Democracies likewise should not avoid such technologies out of fear, but rather harness them responsibly to empower their causes. Deception remains a critical element of warfare, and Western democracies must recognise that using AI strategically – even for controlled deception – can serve as a means to achieve legitimate ends, provided it adheres to ethical standards that distinguish them from authoritarian regimes.

Much like the advent of nuclear weapons marked a pivotal moment in military strategy and governance, AI represents a similar crossroads for the modern world. Democracies must recognise the dual nature of AI: on one hand, it has the potential to empower them, creating resilience and challenging authoritarian regimes; on the other, it can be misused in ways that undermine democratic values. Similarly to nuclear deterrence, where clear policies govern its use, AI requires the same level of strategic clarity. Democratic nations did not, and still do not, shy away from enhancing their nuclear capabilities as part of a broader strategy of deterrence and psychological warfare; why should AI be any different?

AI is not the enemy but a natural evolution of technology. It represents a crossroads for modern governance, in the same way as nuclear weapons did in the 20th century. Its use has both offensive and defensive purposes, yet it must be understood as both a tool of potential empowerment and a weapon with serious consequences if

mishandled. Just as nuclear deterrence led to the creation of strategic policies, AI needs its own framework for responsible use. Democracies did not shy away from nuclear capabilities when it served strategic ends; similarly, AI, when wielded with clarity and ethics, should serve democratic objectives. The importance of the ethical use of AI, then, lies in ensuring that its role in decision-making and societal engagement remains aligned with democratic principles – transparent, accountable, and open to scrutiny.

## Conclusions

AI has become an integral element of global competition across various domains. A particularly pressing challenge is the growing tendency of autocratic regimes to leverage AI technologies to enhance the effectiveness of their disinformation campaigns. While Western nations engage in debates over ethical norms and pursue efforts to establish international regulations for AI, revisionist powers exploit vulnerabilities in the information ecosystems of democracies.



***Much like the advent of nuclear weapons marked a pivotal moment in military strategy and governance, AI represents a similar crossroads for the modern world***

---

Analysis indicates that the most impactful use of AI in media is the production of deepfakes. These manipulative videos, often perceived by the public as entertainment, have already been weaponised by countries such as China, Russia, and others, seeking to revise the existing global order. Deepfakes are particularly effective both as tools of hybrid warfare – commonly employed to influence elections – and as components of

information and psychological operations accompanying threats or acts of armed aggression. Additionally, AI can significantly enhance the adaptability and ‘credibility’ of bots that amplify disinformation on social media platforms.

The threat posed by Russian propaganda in the context of AI adoption warrants special attention, particularly regarding the information security of Western nations. Despite facing economic challenges, Moscow continues to pursue ambitious objectives in AI development. Furthermore, the ongoing war in Ukraine and Russia’s strategic partnership with China may provide additional impetus for the Kremlin to intensify its subversive information activities through the malicious application of AI technologies.

---

**Volodymyr Solovian**, PhD, is Head of the Hybrid Warfare Analytical Group at the Ukraine Crisis Media Centre (UCMC). He holds a PhD in Philosophy from the Taras Shevchenko National University of Kyiv. He previously worked as an expert at the Centre for Army, Conversion and Disarmament. Volodymyr is a specialist in information security, Russian disinformation, and Ukrainian defence policy. He is a member of the Advisory Group of the Political Department of the Ministry of Foreign Affairs of Ukraine.

**Matt Wickham** is an analyst at the Hybrid Warfare Analytical Group at the UCMC. He is a graduate of the UCL School of Slavonic and East European Studies in Russian and Ukrainian Studies. Matt specialises in countering Russian propaganda. He focuses on identifying and analysing hostile influencers and political actors collaborating with Russia.

---

## BOARD OF ADVISORS

**Dr. Dimitar Bechev** (Bulgaria, Director of the European Policy Institute)

**Dr. Iulian Chifu** (Romania, State Counsellor of the Romanian Prime Minister for Foreign Relations, Security and Strategic Affairs)

**Amb., Dr. Sergiy Korsunsky** (Ukraine, Ambassador Extraordinary and Plenipotentiary of Ukraine to Japan)

**Prof., Dr. Igor Koval** (Ukraine, Odesa City Council)

**Felix Hett** (Germany, Director Friedrich Ebert Stiftung Ukraine)

**James Nixey** (United Kingdom, Head of the Russia and Eurasia Programme at Chatham House, the Royal Institute of International Affairs)

**Amb., Dr. Róbert Ondrejcsák** (Slovakia, Ambassador Extraordinary and Plenipotentiary of the Slovak Republic to the United Kingdom of Great Britain and Northern Ireland)

**Amb., Dr. Oleg Shamshur** (Ukraine, former Ambassador Extraordinary and Plenipotentiary of Ukraine to France)

**Dr. Stephan De Spiegeleire** (The Netherlands, Director, Defence Transformation at The Hague Centre for Strategic Studies)

**Ivanna Klympush-Tsintsadze** (Ukraine, Head of the Parliamentary Committee on European Integration)

**Dr. Dimitris Triantaphyllou** (Greece, Professor of International Politics, Panteion University, Athens)

**Dr. Asle Toje** (Norway, Vice Chair of the Nobel Committee, Research Director at the Norwegian Nobel Institute)







UA: UKRAINE  
ANALYTICA

Issue 3 (35), 2024

ISSN 2518-7481