ALGORITHMIC HYBRID WARFARE: AI-DRIVEN DISINFORMATION IN THE RUSSIA-UKRAINE WAR

Muhammad Noman, Mahnoor Azhar and Zeeshan Fida[*]

Abstract

In the contemporary era, the weaponisation of digital platforms for perception and narrative control is becoming a crucial element in the emerging fifth-generation warfare. This paper examines the AI-driven disinformation campaigns during the 2022 Russia-Ukraine war to analyse the impact of modern technologies on armed conflicts. Through a qualitative comparative case study research design, this paper comparatively analyses the asymmetry and reach of Russia and Ukraine's AI-based information operations. The central focus of the research is to understand the extensive use of AI by Russia and Ukraine and its effectiveness in disseminating false narratives and shaping global perception. The research revealed that Russian information operations leveraged advanced technology and possess a broader international reach, whereas the Western-supported Ukrainian countermeasures are more defensive and domestic in nature. The findings suggest that AI is reinventing contemporary warfare while emphasising the decisive role of narrative framing in shaping future conflict outcomes.

Keywords: Artificial Intelligence, Disinformation, Hybrid Warfare, Psychological Operations, Perception, Narrative.

Introduction

The warfare in the twenty-first century has acquired a fifth domain in the form of information operations, and its weaponization was demonstrated in the Russia Ukraine war. The Russia-Ukraine conflict, which began with the annexation of Crimea on 18 March 2014 and dramatically escalated in 2022, highlighted the growing significance of the information domain in modern warfare.[1] Russia and Ukraine have relentlessly employed disinformation strategies such as deepfake videos, coordinated bot networks, false alerts, and fake regional news outlets to shape public opinion and influence the international narrative in their favor. This case study is not an isolated incident; instead, it reveals the evolving nature of warfare strategies by introducing a new frontier alongside land, sea, and air. Artificial Intelligence (AI) has become a strategic tool in the creation, dissemination, and consumption of disinformation during the Russia-Ukraine war, making it a strong case study to highlight the use of modern technologies in military campaigns.

[*]Muhammad Noman is an Independent Research Analyst based in Islamabad. Mahnoor Azhar is also a Research Scholar at the Department of International Relations, Fatima Jinnah Women University, Rawalpindi. Dr Zeeshan Fida is a Lecturer at the Department of International Relations, Fatima Jinnah Women University, Rawalpindi. The authors can be reached at naumanafridi608@gmail.com.

Information operations have traditionally functioned as an integral dimension of strategic policies and armed conflicts. During the Cold War, both the United States and the Soviet Union utilised mass media and radio broadcasts to counter narratives and shape discourse.[2] In the post-Cold War era, hybrid warfare emerged, which marked the fusion of information operations with cyber activities and economic coercion.[3] With the digital revolution, these propaganda techniques became more sophisticated and extensive. Due to the rise of social media platforms, the creation and dissemination of both disinformation and misinformation have become a new normal.[4]

The development and integration of artificial intelligence in the hybrid war have revolutionised this domain by enabling the creation of deepfakes, synthetic media, and automated bots driven narrative framing.[5] The Russia-Ukraine war provided a most consequential live laboratory for AI-driven disinformation campaigns in the contemporary conflicts. Both states used AI-based disinformation strategies, one example is that Russia circulated fabricated pictures of Ukraine committing atrocities on civilians created through AI, to distort international perceptions and undermine Ukrainian resilience.[6] Conversely, Ukraine also used machine intelligence and other related technologies to counter Russian AI-driven disinformation campaigns during the war.[7] A growing body of literature focuses on the Russian and Ukrainian AI-based disinformation strategies in isolation. A systematic comparative analysis of both belligerents' disinformation propaganda techniques and the resulting asymmetric narrative outcomes remains absent from the existing debate.

To bridge this gap in the existing literature, this research is structured around three key questions, focusing on the AI-driven disinformation operations deployed by Russia during the war and the institutional and technological counters employed by Ukraine. Thirdly, this paper answers the comparative impact of these strategies on narrative building and how much they differ in asymmetry and reach. The central argument of this paper is that Russia's AI-enabled disinformation campaigns are more internationally oriented and technologically superior than those of Ukraine, which remain defensive and domestically focused.

The research article has six major sections. A conceptual framework outlines hybrid and psychological warfare as foundational concepts for examining the deployment of AI-based information campaigns by Russia and Ukraine. A methodology section explains the application of a comparative research design. Then, the historical background outlines the evolution of the propaganda used in war over time, followed by a detailed account of Russia's AI-driven disinformation campaign, including the tactical manipulation and globalisation of AI-based propaganda. Further, this paper covers the countermeasures taken by Ukraine against Russian operations. The article concludes with major findings about the competing narratives and asymmetries between Russia and Ukraine in their respective information operations.

Conceptual Framework

Military strategies are evolving with the rise of modern technology and sophisticated weapon systems, reflecting an ongoing Revolution in Military Affairs (RMA). RMA represents a transition from post-industrial warfare to informationized warfare, where data superiority, real-time intelligence, and advanced information operations become a decisive source of military advantage. In modern warfare, states are employing war at a sub-conventional level to weaken an adversary's internal state dynamics. Hybrid warfare defines tactics that infuse both traditional and irregular strategies used by countries to erode the boundary between peace and conflict. In contemporary literature, Frank G. Hoffman characterises hybrid warfare as a nexus of four basic components: conventional capabilities, irregular tactics, terrorism, and organised crime.[8] NATO defines a hybrid threat as a blend of military and non-military methods, disinformation, cyber intrusions, economic pressures, and deployment of irregular and regular armed groups, primarily to influence the minds of the population and destabilise societies.[9] Russia predominantly used hybrid warfare tools and tactics to advance national interests without resorting to full-scale war. One of the manifestations of this in recent history is the Crimean annexation in 2014.

Russia used information operations, cyber-attacks, and proxies to influence political processes and advance the strategic interests of the Kremlin.[10] This research examines the complex dynamics of the Russia-Ukraine war through the conceptual model of hybrid warfare, as both states are employing nontraditional military strategies parallel to conventional war. Russia is increasingly using psychological operations as a tool of hybrid warfare alongside conventional operations to influence enemy morale, civilian perception, and international opinion. Ukraine is countering Russian information operations in a defensive manner by debunking fabricated audio-visual content. These tactics are outlined by NATO as cognitive warfare, where states are trying to manipulate public opinion by influencing the thinking pattern, interpretation of reality, and decision-making.[11] The use of artificial intelligence for disinformation campaigns by both warring parties demonstrates the significance of modern technologies in this war, marking a shift from traditional warfare tactics towards a more technologically advanced form of military contestations. This shift highlights the growing importance of controlling narratives and perceptions through media manipulation as a strategic advantage for states during conflicts.

Research Methodology

This research used a qualitative methodology to understand the role of artificial intelligence in hybrid warfare and disinformation during the Russia-Ukraine war. Through a comparative qualitative case study research design, this paper systematically analyses and contrasts the AI-driven disinformation strategies used by Russia and Ukraine during the war.[12] The data has been drawn from secondary sources and established reports, publications by Atlantic Council, EU DisinfoLab, Nato Strategic Communication Centre, and peer-reviewed literature.

These sources were selected on the basis of institutional credibility, methodological transparency, and direct relevance to AI-driven operations during the Russia-Ukraine war. Telegram, X, and Facebook were selected as primary platforms because these sites were principal arenas for the dissemination of information by both states. The reports and videos are comparatively analysed around four comparison variables: narrative building, AI-driven techniques, platform-specific dissemination patterns, and impact on national and international public perception. The primary limitation of the study is over-reliance on secondary data, which creates the possibility of prior analytical bias.

Historical Context of the Russia-Ukraine Conflict

In the beginning of 2014, Russia annexed Crimea, and a separatist uprising erupted in eastern Ukraine, which triggered the perpetual cycle of hostilities between Russia and Ukraine.[13] Following this, both belligerents shifted towards hybrid warfare tactics, which demonstrates the rapidly evolving nature of contemporary conflicts. The warring parties used both traditional and non-traditional tools, including missile strikes, drone attacks, cyber operations, and disinformation campaigns. NATO's European Commander at the time termed this invasion as the most amazing information warfare. Russian state-controlled media were actively engaged in spreading false narratives about Ukraine and the West.[14] With the full-scale invasion in 2022, the incorporation of AI-driven disinformation and propaganda campaigns has modernised the hybrid warfare techniques. Russia utilised AI-generated disinformation operations to promote its narrative and gain public support. Through social media, they disseminated deep-fake videos of Ukrainian officials surrendering and automated bots to manipulate perceptions.

Previously, propaganda was the dissemination of transparent narratives to manipulate the perceptions of an individual regarding the world. AI has now revolutionised the propaganda techniques by making it faster, more targeted, and more convincing. Smart bots adjust their messages according to the emotional state of the users at the moment, and artificial intelligence edits videos that look official in real-time. Even announcements which are intended to provide people with an official public service message can be twisted. For instance, deepfake voices can redirect civilians to the unsafe routes or report false orders.[15] In other words, AI has made drone cameras, smartphone cameras, and messenger apps a weapon during the Russia-Ukraine war. Disinformation is disseminated to targeted audiences through hyper-personalised false narratives.[16] These disinformation operations transform civilians into participants in the war and destabilise societies by undermining social cohesion and institutional trust. The massive use of digital information tools in the Russia-Ukraine war signals the growing significance of advanced technologies, such as artificial intelligence, in advanced military conflict. These technologies are complicating the process of differentiating between truth and lies, while highlighting the challenge of countering disinformation amid rapidly advancing technology.

Russia's AI-driven Disinformation Campaign

Following the 2014 Russian invasion of Crimea, Moscow framed this as a real uprising by local Crimean residents through disinformation. Russian authorities repeatedly denied the involvement of their armed forces during the Crimean invasion. Various soldiers were identified in Russian-style uniforms, nicknamed "little green men" as they took control of strategic areas in Crimea.[17] The Russian president, Vladimir Putin, also rejected any prospect of Russian military involvement by calling those soldiers local self-defence units. However, it was later revealed that the men in green uniforms were actually Russian soldiers. This disinformation campaign was further optimised through online automated bots and fabricated documents, which portrayed that most Crimeans are in favour of joining Russia. This large-scale disinformation crusade started to distort global understanding of events by 2015, which helped Russia to take full control of Crimea without any organised opposition.

Initially, Russia was waging traditional propaganda, but from 2022 onwards, it has started launching well-organised AI-based disinformation campaigns primarily to damage Ukraine's image and weaken the international support.[18] In the middle of 2022, pro-Russian media channels such as RT and Telegram circulated a video which showed Ukraine's armed forces deliberately targeting civilian communities. [19] Following that, assessments by fact-checking institutions like Bellingcat identified that the video and images were AI-generated.[20] In another event, a fabricated video of Ukrainian President Volodymyr Zelensky was released by Russia in which he was calling for Ukrainian military capitulation, but that was debunked later.[21] Similarly, another disinformation campaign was launched through artificial intelligence that portrayed the Ukrainian armed forces bombing civilian centres to undermine Ukraine's credibility in the global arena, but subsequently, this video was also reported as a deep fake.[22] Such a type of media is produced and disseminated through online platforms, i.e., Telegram, X former Twitter, and Facebook, through AI chatbots to spread disinformation.

Furthermore, news was spread on X and Facebook that Ukraine is establishing manufacturing laboratories for biological weapons. This fake news was disseminated by automatic bots of Russia's cyber team and diffused quickly in the online world. This content most affected states like India and Brazil, where countering such information is difficult. In 2023, Russia used religious sensitivity to trigger the Eastern European population against Ukraine. In this regard, they created a fake video of Ukrainian troops attacking religious worship places, which went viral.[23] Subsequent verification by Reuters' fact-checking team determined that these videos were created through AI with zero authenticity.

To further advance its disinformation efforts, Russia attempted to influence the NATO member states. By using automatic bots, they started spreading fake news articles in Germany, which framed Ukrainian refugees as the main reason for economic hardships.

By 2024, these AI-driven disinformation campaigns of Russia became more effective. A recording of NATO officers went viral on the global stage in 2024, in which they were discussing escalating war with Russia.[24] This video became the centre of public attention, but later, with the help of the Guardian's investigative team, it was exposed as being generated by Russian AI software.

Furthermore, Russia released various documents with fake signatures to propagate the information that Ukrainian officials are using the US and NATO financial support for their luxuries. Following coverage by various European media groups, the European Digital Media Observatory (EDMO) came forward to test its authenticity. After a detailed investigation, they reported that the news was fake and contrary to facts.[25] Similarly, certain LinkedIn accounts operated by automated bots tried to influence European decision-makers. According to reports released by think tanks, these accounts were suggesting that the Ukrainian military was depleted and required additional support. Later, cybersecurity organisation Mandiant verified that the Russian intelligence was spreading these fake reports.

Tactical Manipulation and Psychological Warfare

Russia's information war was increasingly relying on AI to inflict fear and chaos on the ground. Like, coordinated fake evacuation messages, purportedly from Ukrainian authorities, spread across social media, claiming that the citizens in Kharkiv and Zaporizhzhia would be under an immediate threat.[26] Atlantic Council experts pointed out how "sophisticated hoaxes" with Ukrainian government logos showed "safe evacuation routes" and tricked citizens into panic. Meanwhile, voice cloning and deepfake technology also increased significantly, as AI-created video and audio files of officials were being shared on messaging services. These tactics are used by the Russian military as psychological operations to spread chaos and confusion among the Ukrainian population to weaken their resistance. These tools amplify both the scale and diversity of propaganda, enabling its disseminators to produce content in near real-time, generate multiple variations, and make it increasingly difficult to identify as artificial. [27]

The online networks of Moscow in the middle of 2024 started creating fake scenes of disaster, primarily to demoralise the Ukrainian population. In another example, the Counter-Disinfo Centre of Ukraine explored a video used by Russian propaganda media and fully revealed that the so-called video of a doctor spraying fake blood at a bombed hospital was staged.[28] Such hoaxes expose artificial intelligence-based stories that are aimed at blowing up local trust and growing the use of machine intelligence in psychological warfare. Reports by Center for Strategic and International Studies (CSIS), highlight the effect of AI in boosting disinformation.[29] The amount of content created by AI chatbots and tools is significantly higher than what human networks could achieve on their own, which makes disinformation a crisis on a global scale.

Surveys indicate that AI can automatically translate propaganda into multiple languages and generate tailored texts and videos, thereby amplifying the circulation of fake information.

A massive amount of propaganda material was also spread on the Chinese-owned TikTok platform. By late 2024, Ukrainian disinformation experts indicated that TikTok was even worse than Telegram. Tens of thousands of accounts (including those affiliated with Russian state media) pumped AI-generated content into the ears of both young and elderly Ukrainians. Even the Disinfo Centre in Ukraine released lists of potentially harmful TikTok account handles when it partnered with the company to counter rumours powered by AI.[30] Thus, social media apps that were primarily introduced as a tool for spreading amusement also became a source of AI-powered influence. The use of AI to influence people's minds and behaviour during the war demonstrated revolutionary changes in traditional warfare tactics towards more technology-driven operations. These cyber-assisted psychological operations are employed to create fear and confusion among people in order to make them feel weak and hopeless.

Industrialisation and Globalisation of Russian AI Propaganda

By 2024 and 2025, Russian information operations became more sophisticated, centralised, and AI-driven. Kremlin units operate so-called sentiment-aware bot networks to monitor responses in real time, and modify tone and content accordingly, just as in marketing software. Moreover, Moscow has also introduced synthetic media platforms, supposedly AI news services whose animated anchors serve up dozens of languages of Kremlin talking points that are disguised to resemble veritable news. Russia has also extended disinformation even to Asia, Latin America, and Africa. Scientists cite organised Russian-Chinese FIMI actions that have the effect of impacting areas like Latin America and the Asia Pacific.[31] To promote propaganda about the war, AI translation and text-generation are used by state media authorities to introduce local-language conspiracy sites in India and Brazil, amongst other places.

Moreover, Moscow has targeted different people with different messages. The westerners are fed exaggerated messages of danger in Ukraine; the non-aligned countries receive anti-American messages, and the immediate countries on the front read highly localised stories about chaos. With the application of AI, every group receives a personalised campaign. AI producers assemble audio slices in Telegram channels; AI bots tweet multilingual memes; and TikTok accounts use the same AI scripts in their messages to attract various groups of people. The outcome is a type of industrial-scale disinformation apparatus, which sells Russian state narratives to the entire world.[32] By incorporating artificial intelligence, Russia has taken disinformation to the industry level. Depending on the AI tools, propagandists can generate thousands of customised posts or videos within minutes, micro-target warzones and foreign elections alike.

Thus, AI has transformed information into a widely deployed weapon, enabling users in cities like Tokyo or Buenos Aires to unknowingly encounter Kremlin-produced fake content labelled as news.

Ukraine's Strategic Countermeasures to Russian Disinformation

In response to the AI-driven disinformation campaign by Russia, Ukraine has responded defensively with greater coordination and a high-tech plan. The country initiated digital safety by establishing institutions and partnerships that surpass its borders. The Ukrainian initiatives aren't just disproving fake stories, but they are also creating more solid defences among citizens, enhancing media literacy, and forming alliances with large tech companies.

To counter Russian AI-powered information operations, Ukraine also employed modern technologies to expose Russian propaganda. Ukraine established an advanced system, the Ukrainian Centre for Countering Disinformation (CCD), in 2021 and further updated it in 2022. This system was created to track disinformation-based social media trends and content shared through pro-Russia accounts.[33] In 2023, the CDD researchers analysed and debunked the pictures of Ukrainian soldiers desecrating a church as fake, which were circulated by Russia.[34] They also introduced another platform, termed Stop Fake, with the help of Western states and voluntary organisations. The system helped Ukrainian authorities to counter Russian disinformation by scanning the AI-generated material and cross-checking the viral pictures and videos with original content.[35]

AI-Based Counter Disinformation Tools

To identify Russian automatic chatbots, Ukraine has employed highly developed AI technologies. For instance, Ukraine collaborated with a private technical company, Mandiant, to expose bot networks and their activities.[36] During 2023, news spread in Germany and Poland that Ukrainian refugees were responsible for increasing criminal behavior. Using AI-based technologies, Ukraine identified 5000 automated bot accounts in 72 hours and ordered their removal.[37] These measures helped Ukraine to identify and neutralise spurious and AI-generated content, preventing public panic amid the hostilities. Ukraine has further strengthened its counter-disinformation capabilities through collaborations with global tech organisations. Ukraine partnered with Google and Meta in 2023 to enhance its AI models for detecting harmful content. [38] These arrangements played a primary role in identifying Russian propaganda and provided defence to the Ukrainian population against psychological operations. But these initiatives proved to be effective domestically as compared to Russian propaganda, which is technologically superior and globally proliferated, and continues to overshadow Ukraine in neutral states.

In response to Russian propaganda of spreading fake news, Ukraine has changed its strategy from merely protecting itself online to being on the offensive as well. The government, with its technology partners, has introduced high-tech tools in detecting and countering such lies. A tool known as TRUTHNET is one of them. It has Microsoft and Palantir backing, and functions through the analysis of social media streams via AI, to find hoaxes and quickly crowdsources fact-checking.[39]

According to Palantir CEO, Alex Karp, "the US data analytics firm is highly involved in improving the targeting functions, from tanks to artillery, and is responsible for most of the targeting in Ukraine".[40] As a new Russian lie gets distributed, TRUTHNET marks the post right when it sends the signal to officials, informing them about any potential danger of going viral, so that they can break the lie. One example of proactive debunking is the attack on the hospital in Mykolaiv. Fake news was identified through artificial intelligence-based alerts; thus, analysts applied AI image forensics and followed the resources. The Ukrainian media published the truth and released machine-translated transcripts revealing the reality that it was actors posing as doctors, and debunked the lie. [41]

Civilian Centred Information Campaigns

In spreading awareness among its population, Ukraine has organised workshops in the cities of Dnipro and Sumy, where simulation tools are presented to demonstrate how deepfakes are created. These cyber defence drills train individuals to detect voice cloning and edit video. Research indicates thousands of people have attended AI open-source intelligence classes, and they learn to verify suspicious posts within a short time.[42] Ukraine had the forward-looking plan to make its citizens defence nodes by spreading information and knowledge among them, thus the country creates "citizen-soldiers of the information war". The people are informed on how to evaluate the viral posts using public service announcements. Curricula at schools have been revised, and the AI-thinking modules have been added to the national cyber-education plan to be taught to teenagers. What this implies is that rather than simply responding to fake news, Ukraine is planning to foster skepticism in the daily lives of its people.[43]

Ukraine has shifted its strategy regarding fake news circulation from being reactive to proactive, anticipating its emergence and campaigning on it. Cybersecurity is critical just like air defences. The information policy of Ukraine is so far-reaching now: millions of Ukrainians, starting with soldiers and ordinary people, are being taught how to identify fakes using artificial intelligence. The fact that the Ukrainian Head of State has made digital literacy accessible to all citizens, converting them into first responders against disinformation. In a basic sense, the nation is weaponising awareness by making the issue of vulnerability a massive strength corresponding to the supply of military AI advancements.

Competing Narratives and Operational Asymmetry

The Russia-Ukraine war operationalises the twenty-first-century hybrid warfare domain by integrating artificial intelligence-based disinformation campaigns to influence perceptions and narratives during the war. These AI-driven information operations provide a systematic comparison between both warring parties over competing narrative claims, AI- based techniques, social media platforms, and impact on audience perception. From the standpoint of pro-Russian actors, cyber-based AI tools are significant for controlling narratives and countering Western influence.

Russia has utilised artificial intelligence to undermine Ukraine's image and weaken international support. For this purpose, they targeted the Global South primarily to gain anti-Western sympathies from the former colonies of the West. They circulated manipulated media in neutral nations like India and Brazil to establish an anti-Ukraine narrative.[44] Furthermore, Russia tried to spread chaos and panic among the Ukrainian population and military to demoralise them. According to 2023 reports by the European Digital Media Observatory, Russian disinformation campaigns sought to influence European decision-making and undermine support for Ukraine.[45] Whereas, Ukraine was primarily on the defensive side by countering the Russian narratives through debunking truth and realities. Instead of creating alternative realities, Ukraine exposed the Russian fabricated media, which demonstrated that their measures were reactive and transparent.

For spreading this narrative globally, Russia employed various AI-based tools to deliver deepfake recordings, controlled pictures, and bot-driven networks. They also disseminated fabricated documents, fake news articles, AI-based news services, and voice-cloned audio files of officials to spread Russian state propaganda. Russia used social media platforms, including Telegram, Facebook, X, and TikTok, to disseminate fake media around the world. In contrast, Ukraine used counter-disinformation tools by developing media literacy among civilians and creating alliances with tech companies. Ukraine incorporated AI-driven authentication and legal frameworks for media in its response. For example, in the middle of 2024, Ukraine quickly exposed an AI activity and generated small messages claiming that NATO plans to directly intervene in the Ukraine war.[46] Ukrainian platforms like Stop Fake and the Centre for Countering Disinformation use artificial intelligence to analyse trends and counter Russian disinformation. These measures aim to foster Ukraine's credibility and sustain public trust during the conflict. Further, Ukraine emphasised that AI could safely be employed in warfare and encouraged openness and the voice of the citizens to be heard more. Ukrainian officials revealed that AI was not limited to fact-checking; it also saved civilian lives by detecting fake shelter warnings and preventing misinformation that could have panicked them. To promote the efforts, the government initiated campaigns that promoted the concept of the so-called digital sovereignty, encouraging people to view online resources with extra care.[47]

Moscow-backed media approach these activities as efforts to reveal information hidden by the West and Ukraine, to portray Russia as a victim of worldwide propaganda in front of a national and international audience. In 2025, supporters of Russia labelled their AI-driven disinformation as "informational defence." They claim that their strategies are necessary since the Western media and narrative producers have already taken over international discussions.[48] They claim that an AI-enhanced messaging by Russia is just a balancing act by its mass media, since it is possible to influence opinions in the West by selectively choosing facts. This assertion was particularly echoed in Sub-Saharan Africa and Southeast Asia, where distrust in Western institutions is already present.

Through AI, Russian actors declared that they were democratizing truth, and it was Ukraine and its allies who established narrative monopolies rather than advocates of openness.[49] Russia remained successful in keeping the Global South neutral during the war despite pressures from the West. Conversely, Ukrainian countermeasures were primarily focusing on the domestic audience, making them more resilient to disinformation operations through media literacy. International observers acknowledge the sophisticated use of artificial intelligence by both sides and have determined the scale and forcefulness of Russian operations. Russian information operations are more offensive, sophisticated, technologically superior, and have impacted a broader geographical scope. Whereas Ukraine's initiatives are more defensive and geographically constrained at the domestic and regional level, demonstrating a strategic imbalance between the two conflicting parties. Russia has effectively utilised machine intelligence as a hybrid warfare tool for impactful psychological operations and anti-Western narrative building. This dimension of contemporary warfare signifies the transforming nature of technology by pushing traditional military engagement to a low-intensity level.

Conclusion

The Russia-Ukraine war has emphasised the significant impact of artificial intelligence in contemporary information warfare. Russia has used advanced computer-based intelligence tools, including deepfakes and automatic bot accounts, to spread fabricated stories, undermine Ukrainian legitimacy, and influence the international audience. On the other hand, Ukraine has developed robust AI-based defences, such as public awareness campaigns, media-based criminal justice, and fact-checking mechanisms. Comparatively, Russian information operations provided a successful case study of hybrid warfare through information and psychological operations by undermining Ukrainian and Western legitimacy in various parts of the world. An operational asymmetry is evident between Russia and Ukraine, which demonstrates the significance of power dynamics between adversaries in a conflict.

As a powerful country with a strong military and economy, Russia employed more sophisticated and technologically superior disinformation operations against Ukraine around the globe. Ukraine is largely relying on Western states for countering Russia across conventional and informational arenas.

The Russia-Ukraine war signals a substantial transformation in traditional warfare. The success is no longer guaranteed through advanced weaponry and well-trained troops; instead, perceptions and narratives are becoming decisive factors. There are two large concepts about who owns the narrative and who can propagate quickly. The reality is difficult to comprehend with daily streams of AI-based content. This poses a danger to national security as well as reducing the trust of the people. With deepfakes becoming more realistic and AI-aided stories appearing in real-time, countries will have to shift the focus to offensive rather than defensive strategies.

To counter the threats posed by AI-based disinformation operations, states must formulate both domestic and international responses. At the national level, states can build a resilient society through enhanced digital literacy among civilians, as Ukraine did to counter Russian offensives. For this purpose, states can introduce a school curriculum to teach students about the growing use of AI for disinformation and how to comprehend the fake and real information. States can also educate civilians through media awareness workshops and fact-checking mechanisms to make them resilient against deepfakes and bot-driven propaganda. At the international level, states should cooperate through multilateral channels to develop global norms and regulatory frameworks that govern the use of AI in warfare. The norms should discourage the use of AI-based deceptive content, primarily to target civilians as a tool of psychological operations, and promote transparency and accountability. Both Russia and Ukraine have demonstrated that future wars will be fought not only with military weapons, but also on feeds, timelines, and screens; thus, the victor in the battle will be determined by who has control over the narratives.

References

[1] Iryna Kovalska-Pavelko et al., "The Russian-Ukrainian War of 2014–2022: A Historical Retrospective," *Cuestiones Políticas* 40, no. 74 (2022): 648-661, https://www.researchgate.net/publication/365309359_The_Russian-Ukrainian_War_of_2014-2022_A_Historical_Retrospective.

[2] Nihila Premakanthan, "Information Warfare Through the Ages: Techniques and Impacts," *ResearchGate*, September 2024, https://www.researchgate.net/publication/384324727_Information_Warfare_Through_the_Ages_Techniques_and_Impacts.

[3] Marco Marsili, "Cognitive Warfare in Historical Perspective: From Cold War Psychological Operations to AI-Driven Information Campaigns," *Preprints.org*, December 17, 2025, https://www.preprints.org/manuscript/202512.1596.

[4] Zoë Adams et al., "(Why) Is Misinformation a Problem?" *Perspectives on Psychological Science* 18, no. 6 (November 2023): 1436–63, https://journals.sagepub.com/doi/10.1177/17456916221141344.

[5] Andrii Paziuk et al., "Decoding Manipulative Narratives in Cognitive Warfare: A Case Study of the Russia-Ukraine Conflict," *Frontiers in Artificial Intelligence* 8 (2025): 1566022, https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1566022/full.

[6] Olena Kuznetsova, "Feature of Russian Disinformation Created by AI on the Internet Media, Social Networks," *Bulletin of Lviv Polytechnic National University: Journalism* 1, no. 7 (2024): 79-89, https://science.lpnu.ua/sjs/all-volumes-and-issues/number-1-7-2024/feature-russian-disinformation-created-ai-internet-media.

[7] Halyna Padalko, "AI for Freedom: Ukraine's Digital Strategy in the Information War," *Forum for Ukrainian Studies*, November 28, 2025, https://ukrainian-studies.ca/2025/11/28/ai-for-freedom/.

[8] Frank G. Hoffman, *Conflict in the 21st Century; The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 5-7, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[9] Tarik Solmaz, "Hybrid Warfare: A Dramatic Example of Conceptual Stretching," *National Security and the Future* 23, no.1 (2022): 89-102, https://www.nsf-journal.hr/NSF-Volumes/Focus/id/1370/p.

[10] Christopher C. Chivvis, "*Understanding Russian 'Hybrid Warfare' and What Can Be Done About It*," testimony before the Committee on Armed Services, United States House of Representatives, March 22, 2017, RAND Corporation, Santa Monica, CA, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.

[11] NATO Allied Command Transformation, "Cognitive Warfare," *Allied Command Transformation*, accessed January 20, 2026, https://www.act.nato.int/activities/cognitive-warfare/.

[12] Marcelo Parreira do Amaral, "Comparative Case Studies: Methodological Discussions," In *Landscapes of Lifelong Learning Policies across Europe*, ed. Sebastiano Bessano, Dejana Bouillet, Tiago Neves, and Marcelo Parreira do Amaral (Cham: Palgrave Macmillan, 2022), 41-60, https://link.springer.com/chapter/10.1007/978-3-030-96454-2_3.

[13] Pavelko et al., "The Russia-Ukraine of 2014-2022."

[14] Yevgeniy Golovchenko, Mareike Hartmann, and Rebecca Adler-Nissen, "State, Media, and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation," *International Affairs* 94, no.5 (2018): 975-994, https://academic.oup.com/ia/article/94/5/975/5092080.

[15] Vincenzo Ciancaglini, Craig Gibson, and David Sancho, "Malicious Uses and Abuses of Artificial Intelligence," *Trend Micro Research for the United Nations Interregional Crime and Justice Research Institute*, November 19, 2020, https://unicri.org/sites/default/files/2020-11/Abuse_ai.pdf.

[16] Roman Osadchuk, "AI Tools Usage for Disinformation in the War in Ukraine," *DFRLab*, July 9, 2024, https://dfrlab.org/2024/07/09/ai-tools-usage-for-disinformation-in-the-war-in-ukraine/.

[17] Steven Pifer, "Watch Out for Little Green Men," *Brookings*, July 7, 2014, https://www.brookings.edu/articles/watch-out-for-little-green-men/.

[18] "Russia-Ukraine Disinformation Tracking Center," *NewsGuard*, accessed January 25, 2026, https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/.

[19] Mamoun Alazab and Kate Macfarlane, "Why Telegram - Despite Being Rife with Russian Disinformation - Became the Go-to App for Ukrainians," *Nieman Lab*, March 29, 2022, https://www.niemanlab.org/2022/03/why-telegram-despite-being-rife-with-russian-disinformation-became-the-go-to-app-for-ukrainians/.

[20] Maxim Edwards, "Russia's Assault on Daily Life in Ukraine," *Bellingcat*, February 24, 2023, https://www.bellingcat.com/news/2023/02/24/russias-assault-on-daily-life-in-ukraine/.

[21] Matyáš Boháček and Hany Farid, "Protecting world leaders against deep fakes using facial, gestural, and vocal mannerisms," *Proceedings of the National Academy of Sciences* 119, no. 48 (2022), https://www.pnas.org/doi/10.1073/pnas.2216035119.

[22] Magdalene Karalis, "Fake leads, defamation and destabilization: how online disinformation continues to impact Russia's invasion of Ukraine," *Intelligence and National Security* 39, no. 3 (2024): 1-10, https://www.researchgate.net/publication/379198681_Fake_leads_defamation_and_destabilization_how_online_disinformation_continues_to_impact_Russia's_invasion_of_Ukraine.

[23] Danielle Ong, "Ukraine Says Russia 'Staged' The Video Showing Ukrainian Soldiers Desecrating Muslim Quran," *International Business Times*, March 17, 2023, https://www.ibtimes.com/ukraine-says-russia-staged-video-showing-ukrainian-soldiers-desecrating-muslim-quran-3677797.

[24] The Ministry of Foreign Affairs of the Russian Federation, *"NATO publication 'NATO-Russia: setting the record straight' debunked"* (press release, November 30, 2021), Russian Mission to the European Union, https://russiaeu.mid.ru/en/press-centre/news/nato_publication_nato_russia_setting_the_record_straight_debunked/.

[25] Sergio Hernandez and Jorge Ocana, "Pro-Russian Manipulation Campaign Seeks to Dissuade Foreigners from Combating on Behalf of Ukraine," *European Digital Media Observatory*, October 29, 2024, https://edmo.eu/publications/pro-russian-manipulation-campaign-seeks-to-dissuade-foreigners-from-combating-on-behalf-of-ukraine/.

[26] Maria Avdeeva, "Bombs and Disinformation: Russia's Campaign to Depopulate Kharkiv," *Atlantic Council*, April 29, 2024, https://www.atlanticcouncil.org/blogs/ukrainealert/bombs-and-disinformation-russias-campaign-to-depopulate-kharkiv/.

[27] Andrew Schwartz and Tiffany Hsu, "Distrust of Everything: Misinformation and AI," July 18, 2023, in *The Truth of the Matter,* produced by Center for Strategic and International Studies, podcast, MP3 audio, 17:54, https://www.csis.org/podcasts/truth-matter/distrust-everything-misinformation-and-ai.

[28] "Ukraine Debunks Fake Russian Propaganda Video of Doctor at Site of Attack on Kyiv Children's Hospital – Video," *Ukrainska Pravda*, July 20, 2024, https://www.pravda.com.ua/eng/news/2024/07/20/7466639/.

[29] "Distrust of Everything: Misinformation and AI"

[30] Daryna Antoniuk, "TikTok More Dangerous to Ukraine Than Telegram, Say Local Disinformation Experts," *The Record from Recorded Future News*, October 3, 2024, https://therecord.media/tiktok-more-dangerous-ukraine-telegram.

[31] Tamás Matura, "Sino-Russian Convergence in Foreign Information Manipulation and Interference: A Global Threat to the US and Its Allies," *Center for European Policy Analysis*, June 30, 2025, https://cepa.org/comprehensive-reports/sino-russian-convergence-in-foreign-information-manipulation-and-interference/.

[32] Matura, "Sino-Russian Convergence in Foreign Information Manipulation and Interference"

[33] National Security and Defence Council of Ukraine, "To overcome the enemy's lies: Center for Countering Disinformation has been operating for over 4 years," 7 May, 2025, https://www.rnbo.gov.ua/en/Diialnist/7169.html.

[34] Stanislav Kovalskyi, "Countering Russian Disinformation and Propaganda in the Ukrainian Information Space (On the Example of the Electronic Resource of the Center for Countering Disinformation at the NSDC of Ukraine)," *Dialog: Media Studios*, no. 29 (2024): 96-108, https://doi.org/10.18524/2308-3255.2023.29.300638.

[35] Lydia Tomkiw, "For Ukraine's Wartime Fact-Checkers, the Battle Rages On," *The Wilson Quarterly*, Winter 2018, https://www.wilsonquarterly.com/quarterly/the-disinformation-age/for-ukraines-wartime-fact-checkers-the-battle-rages-on/.

[36] Andy Greenberg, "Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless," *WIRED*, November 10, 2022, https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/.

[37] The Kyiv Independent News Desk, "SBU, Police Disband 9 Bot Farms Spreading Disinformation," *The Kyiv Independent*, May 3, 2023, SBU, police disband 9 bot farms spreading disinformation.

[38] Kelvin Chan, "Europe Call for Tech Companies to Fight Disinformation by Labeling AI-generated content," *PBS News*, June 5, 2023, https://www.pbs.org/newshour/science/europe-calls-for-tech-companies-to-fight-disinformation-by-labeling-ai-generated-content.

[39] Vera Bergengruen, "How Tech Giants Turned Ukraine into an AI War Lab," *TIME*, February 8, 2024, https://time.com/6691662/ai-ukraine-war-palantir/.

[40] Ulrike Franke and Jenny Söderström, "Star Tech Enterprise: Emerging Technologies in Russia's War on Ukraine," *European Council on Foreign Relations*, September 5, 2023, https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/.

[41] "Fake About the Aftermath of Air Defense in Mykolaiv," *Center for Countering Disinformation*, April 10, 2025, https://cpd.gov.ua/en/international-threats-en/usa/fake-about-the-aftermath-of-air-defense-in-mykolaiv/.

[42] "Ukrainians Eager to Adopt New Technology to Verify Information," *International Media Support*, June 25, 2025, https://www.mediasupport.org/news/ukrainians-eager-to-adopt-new-technology-to-verify-information/.

[43] Peter Schrijver, "Ukraine's Fight on the Front Lines of the Information Environment," *Modern War Institute*, December 9, 2023, https://mwi.westpoint.edu/ukraines-fight-on-the-front-lines-of-the-information-environment/.

[44] Kollen Post, "Ukraine and the Frontlines of the War on Disinformation," *Foreign Policy Research Institute*, August 1, 2024, https://www.fpri.org/article/2024/08/ukraine-and-the-frontlines-of-the-war-on-disinformation/.

[45] Hernandez, "Pro-Russian Manipulation Campaign"

[46] Margarita Konaev, "Tomorrow's Technology in Today's War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability," *CNA | National Security Analysis*, February 10, 2023, https://www.cna.org/reports/2023/10/ai-and-autonomous-technologies-in-the-war-in-ukraine.

[47] "Ukraine is Digital by Design: Resilience and Trust, Embedded in Governance," *E-Governance Academy*, July 2, 2025, https://ega.ee/ukraine-digital-by-design/.

[48] David Gilbert, "A Pro-Russia Disinformation Campaign Is Using Free AI Tools to Fuel a 'Content Explosion'," *WIRED*, July 1, 2025, https://www.wired.com/story/pro-russia-disinformation-campaign-free-ai-tools/.

[49] Emmanuel Grynszpan, "The Russian Disinformation Machine, a Constantly Changing Ecosystem," *Le Monde*, October 12, 2024, https://www.lemonde.fr/en/international/article/2024/10/12/the-russian-disinformation-machine-a-constantly-changing-ecosystem_6729193_4.html.