Commentary #15

David Dondua

Russia's AI Offensive and Europe's Cognitive Defence

The opinions and conclusions expressed are those of the author and do not necessarily reflect the views of the EU Awareness Centre.

© [2025] EU Awareness Centre. All rights reserved.

November 2025

Russia's AI Offensive and Europe's Cognitive Defence

Introduction

At an early stage of its development Artificial Intelligence (AI) was mainly considered to facilitate analysis and communication. Today, AI is often used to influence opponents, spread propaganda, and gain strategic advantages, thus reinforcing traditional combat operations. From automating fake news to guiding information campaigns, AI blurs the line between digital and physical warfare, making control over information as important as control over territory (UNGA, 2025)[i].

Russia's Digital Propaganda: AI as a Weapon of Influence

Such a transformation of artificial intelligence would have been inevitable, although this process was accelerated by Russia's full-scale invasion of Ukraine. From state-controlled broadcasters like *RT* and *Sputnik* to covert networks on Telegram, Facebook, and X, Russia orchestrates an ecosystem of deception aimed at fracturing Western unity and eroding trust in democratic institutions. Nowadays, disinformation has become a core Kremlin weapon, with false narratives spanning every topic, from human rights to civilian bombings, designed to advance Moscow's strategic goals (U.S. Department of State, 2024)[ii].

Early in 2022, Russian channels spread fabricated videos allegedly showing Ukrainian forces committing atrocities in Donbas that were synthetically altered with AI tools to create false "evidence" (Osadchuk, 2024)[iii]. Later, the 2023–2024 "Doppelganger" campaign, traced to Russian-linked actors, used AI-generated replicas of *The Guardian* and *Der Spiegel* websites to post fake stories accusing Ukraine of organ trafficking and NATO of escalation (USCYBERCOM, 2024)[iv]. Distributed via bot networks and Telegram channels, these narratives reached millions before fact-checkers could respond.

By 2025, Russia's propaganda infrastructure had become industrialised through the use of generative AI (Wallner, Copeland, & Giustozzi, 2025)[v]. Automated farms produce thousands of fake articles, cloned voices, and deepfake videos within hours. One striking case was a deepfake of President Zelensky "calling on Ukrainian troops to surrender," which briefly appeared on hacked Ukrainian media before being debunked. Such operations show how propaganda has shifted from handcrafted lies to mass-produced digital forgeries tailored to specific audiences (Boháček & Farid, 2022)[vi].

This industrialisation makes lies faster, cheaper, and harder to trace. AI can generate realistic visuals and texts in multiple languages, overwhelming verification systems and diplomatic communication. Democracies are often forced into a reactive posture, responding to lies rather than setting their own narratives. In Moscow's hybrid strategy, AI has become a weapon of cognitive warfare, used to paralyse decision-making, deepen polarisation, and turn the free flow of information into a vulnerability.

Traditional state tools, such as press releases, briefings, and official statements, cannot match the speed, scale, and precision of AI-driven propaganda. Each manipulated image, headline, or video acts as a force multiplier, shaping perceptions, undermining morale, and influencing strategic decisions. In today's conflicts, information itself is a weapon, and defending truth has become an essential battlefield task, as critical to national security as air defence, artillery, or cyber operations.

Russia's AI Bot Farms: From Human Trolls to Autonomous Influence Machines

In parallel with these high-profile deepfake and media-cloning operations, Russia has also transformed its traditional bot farms into autonomous ecosystems of AI-driven commentators. According to Imperva's 2024 *Bad Bot Report* (Imperva, 2024)[vii], automated online activity surpassed

human activity for the first time in the history of the internet and this shift is largely driven by generative AI. Russian bot operations, once staffed by paid "Olgino" trolls following scripted instructions, are now almost fully automated. Instead of low-skilled workers copying talking points, advanced language models generate millions of adaptive, human-like comments across social networks, capable of engaging in discussions, adjusting tone, and producing convincing text in multiple languages. These AI systems operate continuously, at negligible cost, and scale the Kremlin's narrative warfare far beyond what human labour ever allowed (Dukach, 2025)[viii].

Recent investigations by OpenMinds and DFRLab illustrate the scale of this new threat: more than 3,600 Russian-controlled bots produced over 316,000 comments in Telegram channels across occupied Ukrainian territories in just 18 months, with each bot deploying dozens of narratives from praising occupation authorities to demonising Ukrainian forces. Many of these same accounts reappeared in Moldova, where ahead of the 2025 parliamentary elections they generated over 80,000 comments aimed at discrediting pro-EU parties and creating a false impression of widespread pro-Russian sentiment. Thanks to generative AI, nearly 95% of these comments were unique and contextually tailored to each post, making manual detection nearly impossible. This industrial-scale manipulation fabricates the illusion of a social consensus, pushing undecided citizens toward what appears to be the "majority view", even when that majority is entirely artificial (Dukach, 2025)[ix].

Ukraine's AI-Powered Digital Defence

While democratic governments cautiously explore AI for policy analysis and strategic forecasting, such as the 2024 study by Germany's SWP (Stanzel & Voelsen, 2022)[x], authoritarian regimes have already weaponised it. Democracies are now compelled to adopt AI defensively to detect manipulation, secure information, and preserve diplomatic credibility.

Social media platforms provide tools for engagement, public opinion analysis, and information dissemination. AI enhances these by tracking trends, identifying falsehoods, and enabling targeted outreach. Ukrainian startups Osavul and Mantis Analytics exemplify this new digital deterrence. Born of the war, they utilise large language models (LLMs) and natural language processing (NLP) to detect and analyse disinformation in real time. Working with Ukrainian government agencies, they counter propaganda by spreading verified information faster than lies can circulate, thus turning innovation into a form of cognitive defence (Sobchuk, 2024)[xi].

Other Ukrainian initiatives reinforce this digital resilience. Platforms like Molfar leverage AI and open-source intelligence to monitor propaganda and investigate war crimes, while YouScan analyses social media trends to detect emerging disinformation. Fact-checking initiatives such as StopFake debunk false narratives and disseminate verified information across multiple channels. Together, all these tools create a coordinated AI-driven defence against Russian disinformation (PBS, 2022; StopFake, n.d.; Ukrainer, 2022).[xii]

AI Disinformation as a Continental Threat: Securing Europe's Information Space

Russia's AI-powered information operations are not confined to Ukraine; they increasingly target Europe itself. From manipulating narratives around EU enlargement and security policies to spreading divisive content in domestic politics, these campaigns aim to erode trust in European institutions, polarize societies, and amplify extremist movements. The cross-border nature of digital platforms allows a single AI-driven campaign to simultaneously influence multiple countries, undermining the cohesion and credibility of the European project. European citizens are often unaware that the apparent "majority opinion" online may be the product of industrial-scale AI manipulation, creating a distorted perception of consensus.

For Europe, defending against AI-driven disinformation requires a coordinated, multi-layered approach. Beyond national cyber defences and law enforcement, the EU must invest in technological tools capable of detecting automated campaigns, support independent media and fact-checking initiatives, and foster digital literacy among citizens. By combining innovation with regulatory frameworks and public awareness, Europe can transform the challenge of AI disinformation into an opportunity to reinforce democratic resilience, ensuring that the continent's societies remain informed, connected, and resistant to manipulation.

Conclusion: Defending Truth on the Digital Frontline

The battle for truth is now a frontline of modern conflict. Russia's weaponisation of AI shows that control over information, not just territory, drives strategic power. Democracies must defend the objective truth with the same urgency as they would on any battlefield.

Transparency, education, and international cooperation are as vital as tanks or missiles. AI ethics, strategic foresight, and information security have become core tools of defence. Only through technological capability, ethical clarity, and coordinated action can democratic societies withstand the digital onslaught and safeguard their strategic interests.

---

[i] UN General Assembly. (2025). *Artificial Intelligence in the military domain and its implications for international peace and security* (Report of the Secretary-General, A/80/78) [PDF]. https://documents.un.org/doc/undoc/gen/n25/107/66/pdf/n2510766.pdf

[ii] U.S. Department of State. (2024, February 8). *Disarming disinformation: Our shared responsibility.* https://2021-2025.state.gov/disarming-disinformation/?safe=1

[iii] Osadchuk R. (2024). AI tools usage for disinformation in the war in Ukraine. DFRLab. AI tools usage for disinformation in the war in Ukraine - DFRLab

[iv] USCYBERCOM. (2024). Russian Disinformation Campaign "DoppelGänger" Unmasked: A Web of Deception. Russian Disinformation Campaign "DoppelGänger" Unmasked: A Web of Deception > U.S. Cyber Command > News

[v] Wallner C., Copeland S., & Giustozzi A. (2025). Russia, AI and the Future of Disinformation Warfare. RUSI. Russia, AI and the Future of Disinformation Warfare

[vi] Boháček, P., & Farid, H. (2022). *Deepfakes and disinformation: Challenges for democratic societies*. Journal of Strategic Studies, 45(6), 987–1012.

[vii] Imperva. (2024). *2024 Bad Bot Report* [PDF]. Imperva. https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/

[viii] Dukach, Y. (2025, November 21). *Армия комментаторов. Как ИИ превратил российские ботофермы в оружие влияния.* Українська правда. https://www.pravda.com.ua/rus/articles/2025/11/21/8008280/

[ix] Ibid.

[x] Stanzel V. & Voelsen D. (2022). Diplomacy and Artificial Intelligence. Reflections on Practical Assistance for Diplomatic Negotiations. WSP Research Paper. Diplomacy and Artificial Intelligence. Reflections on Practical Assistance for Diplomatic Negotiations

[xi] Sobchuk M. (2024). How Ukraine uses AI to fight Russian information operations. Global Governance Institute. How Ukraine uses AI to fight Russian information operations

[xii] PBS. (2022). *Ukrainian company uses social media, open-source technology to counter Russian invasion.* https://www.pbs.org/newshour/show/ukrainian-company-uses-social-media-open-source-technology-to-counter-russian-invasion; Ukrainer. (2022). *How Ukraine's civil society battles Russia in the information war.* https://www.ukrainer.net/en/how-ukraine-s-civil-society-battles-russia-in-the-information-war

David Dondua

Ambassador David Dondua is a diplomat and expert in international security, conflict resolution, and European integration. During his diplomatic career in the Georgian foreign service (1993–2022), he held key positions, including Ambassador to Austria, Greece, and NATO. Beyond diplomacy, he has been an associate professor and lecturer at various universities. He currently represents the European Public Law Organisation (EPLO) at the International Anti-Corruption Academy (IACA) in Vienna. He serves as Chairman of the Board of Directors of the EU Awareness Centre.