# Pro-Russian blogs in Europe and UK use AI to flood online space with Kremlin narratives ahead of 2024 elections



Over the past year, pro-Russian narratives have intensified online, particularly across blogging platforms like Substack and various personal websites, primarily authored by individuals based in the UK and Europe. This surge reflects a troubling trend wherein narratives closely mirroring Kremlin messaging are increasingly disguised as independent analysis or personal commentary.

An analytical review reveals a striking consistency among these blogs, which frequently publish near-identical content blaming NATO for the Ukraine conflict, disparaging Ukrainian leadership, and portraying the European Union as self-sabotaging. The near-daily output of these posts suggests a level of coordination that raises suspicions regarding the authenticity of their independence. The systematic replication of these themes indicates a possible reliance on deliberate Kremlin talking points or, potentially, a shared support network.

Moreover, the frequency of posts raises questions about the authenticity of such prolific output. For many solo bloggers, consistently producing well-structured, lengthy articles would be a considerable challenge. However, these bloggers appear to maintain not only volume but also a consistent narrative arc, suggesting the strong possibility of AI-generated content. The usual signs, such as repetitive phrasing and awkward syntax, hint at the employment of language models like ChatGPT for mass-producing these narratives.

The incorporation of AI-generated content poses significant risks in the digital information landscape. The formulaic style and saturation of pro-Russian messages contribute to an overwhelming online presence, creating an illusion of widespread grassroots support for these narratives. This manipulation is strategically designed to create a façade of legitimacy, thereby blurring the lines between genuine dissent and orchestrated propaganda.

Interestingly, some bloggers have opted to switch to Russian when discussing certain contentious issues, particularly those framing Ukraine as neo-Nazi or critiquing Western military aid. While most content remains in English, this linguistic shift targets Russian-speaking audiences, reinforcing connections to the Kremlin's domestic propaganda aims. This dual-lingual strategy enhances the narratives' authenticity and effectively reaches both local and diasporic audiences.

An unsettling question emerges: are these bloggers unwittingly contributing to disinformation efforts, or are they knowingly amplifying state-sponsored narratives? The uniformity of messaging and the capability to generate high-frequency content suggest a more deliberate engagement with disinformation strategies. Whether motivated by ideology, financial incentives, or direct links to pro-Kremlin networks, these writers are undeniably functioning as force multipliers within the broader disinformation narrative.

The cumulative effect of this coordinated blogging is a distorted information landscape that shapes reader perceptions, often without their awareness of the origins of the content. This technique of saturation serves not only to mislead but also to challenge the notion of democratic discourse by reinforcing misleading narratives under the guise of independent observation.

This wave of pro-Russian blogs represents not a spontaneous movement but a calculated effort to undermine the conventional information ecosystem. The patterns of output, combined with the strategic use of AI and language manipulation, point to a sophisticated campaign of information warfare that is undermining trust in democratic institutions and societal cohesion.

The implications of these tactics extend beyond mere propaganda; they actively seek to destabilise public trust in democratic processes, particularly in light of upcoming European elections set to take place in June 2024. As 360 million voters prepare to select their representatives, concerns mount over possible foreign interference and disinformation campaigns. The introduction of the Digital Services Act intends to address these pressing issues, yet challenges persist, especially as emerging technologies heighten the potential for deception.

Europe continues to confront a barrage of disinformation efforts from Russia, exemplified by notorious operations such as deepfake videos and coordinated networks designed to erode public confidence. As concerns about the integrity of electoral processes grow, the need for increased vigilance, regulatory measures, and public awareness becomes ever more critical. The unfolding situation exemplifies the precarious balance between freedom of expression and the safeguarding of democratic values in an increasingly complex and interconnected digital landscape.

### Reference Map

1. Paragraphs 1, 2, 3, 4, 5, 6
2. Paragraph 7
3. Paragraph 8
4. Paragraph 9
5. Paragraph 10
6. Paragraph 11

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://ukdefencejournal.org.uk/the-new-wave-of-russian-disinformation-blogs/> - Please view link - unable to able to access data
2. <https://www.ft.com/content/2ffe8b64-f9bc-46d4-bf40-eefbbc6fac77> - Europe is confronting a surge of disinformation from Russia aimed at undermining support for Ukraine and interfering with EU elections. A notable example involved a deepfake video falsely claiming that French President Emmanuel Macron canceled a trip to Kyiv due to an assassination plot, which went viral after being posted by former Russian president Dmitry Medvedev. European officials are calling for increased vigilance and tougher penalties for online platforms to counter these campaigns. The European Commission plans to introduce stricter disinformation rules soon. Russia's disinformation tactics include creating multiple 'mirror sites' to bypass bans and conducting hybrid operations that merge real-world actions with online propaganda. French cybersecurity efforts have identified coordinated disinformation networks and fake news websites. The disinformation campaigns aim to erode public trust and destabilize European societies, weaponizing both false and genuine information.
3. <https://www.reuters.com/world/us/us-justice-dept-says-it-disrupted-russian-social-media-influence-operation-2024-07-09/> - The U.S. Justice Department announced it had disrupted a Russian social media influence operation aimed at covertly spreading pro-Kremlin messages in the U.S. and abroad. This operation, involving fake social media accounts enhanced by AI, was revealed just four months prior to the U.S. presidential election. The Justice Department secured court orders to seize two domain names and search almost 1,000 social media accounts linked to the scheme. This marks the first public U.S. accusation of a foreign power using generative AI in an influence operation. The campaign was reportedly orchestrated by a Russian private intelligence organization, funded by the Kremlin, and utilized an AI platform to manage fake accounts mimicking Americans. These accounts, now banned, promoted pro-Kremlin content and criticized the Ukrainian government. The operation was run from a server in the Netherlands, with cooperation from Dutch authorities.
4. <https://apnews.com/article/43b7e4017825d9d382859894b7625e7a> - Expert warnings suggest that artificial intelligence could significantly enhance the spread of fake news and disinformation during the upcoming European Union elections, potentially disrupting the democratic process across 27 nations. With around 360 million voters set to elect 720 lawmakers, there are fears that AI tools facilitating the creation of deceptive content will make it easier to mislead voters. Russia and to a lesser extent China are suspected of being behind some of these disinformation campaigns aimed at undermining democracy and stability in Europe. Recent examples include fake websites, bomb threats, and AI-generated content impersonating political figures. The EU has introduced the Digital Services Act to mitigate these risks, compelling tech companies to address disinformation. Platforms like Meta, TikTok, and Google are ramping up measures to protect election integrity, while Elon Musk's X has taken a different approach by disbanding its election integrity team.
5. <https://www.lemonde.fr/en/pixels/article/2024/04/12/european-elections-are-particularly-at-risk-of-foreign-interference_6668197_13.html> - With the European elections scheduled from June 6 to 9, 2024, 360 million voters will be called to the polls to elect their deputies. This critical period is an opportunity for disinformation campaigns and foreign interference, particularly pro-Russian ones. Several European intelligence services have recently denounced propaganda operations targeting their countries. Notable examples include the 'Voice of Europe' corruption network in Poland and the Czech Republic, and 'RRN' or 'Doppelgänger' in France. The historically low voter turnout makes small nations particularly vulnerable. The EU's Digital Services Act (DSA), intended to improve moderation of large platforms, will be tested during these elections. Experts also warn against scenarios like the Slovakian case, where deepfakes and other AI-generated tools could significantly influence voters. Efforts in content detection and labeling, as announced by Meta, will be crucial to counter these threats during the electoral period.
6. <https://www.reuters.com/world/europe/friedrich-merz-targeted-by-pro-russian-disinformation-before-german-vote-2025-02-20/> - Researchers have discovered a network of over 700 fake social media accounts spreading pro-Russian disinformation against Friedrich Merz, the conservative frontrunner in Germany's upcoming election. Dubbed 'Geist,' this bot network promotes anti-conservative messages and AI-generated depictions of Merz, who supports Ukraine in its war with Russia. Merz's support has weakened recently, with the far-right Alternative for Germany (AfD) gaining traction. These accounts began posting anti-Merz content a week before the election, after previously posting non-political content. Germany's cybersecurity watchdog, BSI, is aware of such disinformation campaigns, but the identities behind these accounts remain unclear. While the campaign has seen little engagement, it underscores the efforts to influence the election, which could impact Germany's political landscape and its stance on Ukraine.