Centre for International Governance Innovation

Digital Policy Hub

Digital Policy Hub – Working Paper

AI and Information Manipulation: Russia's Interference in the US Elections

Halyna Padalko

Fall 2024 cohort

About the Hub

The Digital Policy Hub at CIGI is a collaborative space for emerging scholars and innovative thinkers from the social, natural and applied sciences. It provides opportunities for undergraduate and graduate students and post-doctoral and visiting fellows to share and develop research on the rapid evolution and governance of transformative technologies. The Hub is founded on transdisciplinary approaches that seek to increase understanding of the socio-economic and technological impacts of digitalization and improve the quality and relevance of related research. Core research areas include data, economy and society; artificial intelligence; outer space; digitalization, security and democracy; and the environment and natural resources.

The Digital Policy Hub working papers are the product of research related to the Hub's identified themes prepared by participants during their fellowship.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Partners

Thank you to Mitacs for its partnership and support of Digital Policy Hub fellows through the Accelerate program. We would also like to acknowledge the many universities, governments and private sector partners for their involvement allowing CIGI to offer this holistic research environment.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Key Points

- Russia emerges as the most active foreign meddler in US elections, deploying artificial intelligence (AI)-driven disinformation campaigns at scale. Key AI-enabled tactics include narrative manipulation (using generative text, images, deepfakes or cloned voices to produce inflammatory or misleading content), identity falsification through generated profile pictures and bogus news websites, amplification via bot farms and algorithmic manipulation, and strategic targeting that tailors messages to specific communities, thus magnifying social divisions and undermining public trust.
- The rise of generative AI has shifted the disinformation battlefield from primarily influencing human audiences to deliberately "grooming" large language models (LLMs). By flooding the digital sphere with pro-Kremlin narratives, Russia and allied networks aim to contaminate AI training data sets, causing chatbots to repeat or legitimize propaganda.
- Canada should adopt a coordinated policy approach to combat AI-driven information manipulation by consolidating existing legislation into a cohesive framework, enhancing transparency and accountability for social media platforms and LLM developers. Regulatory obligations must include data access for researchers, public reporting and data quality standards, backed by strong enforcement mechanisms.
- The government should support research initiatives and data-sharing collaborations to monitor the evolving information landscape and identify threats in real time. Investing in developing a national LLM, through Canadian platforms such as Cohere, would ensure technological sovereignty, data security and sectoral innovation. Finally, free misinformation media and digital literacy training and dedicated academic programs are essential to build long-term public resilience against disinformation.

Introduction

Rooted in classical strategic theory, Russia's contemporary doctrine of information warfare employs non-kinetic strategies — disinformation, cyberwarfare and psychological operations — to exploit democratic vulnerabilities and avoid the costs of conventional warfare, reflecting a model of "hybrid" warfare (Thomas 2014; Pomerantsev 2014; Fridman 2018). These tactics, traceable to Soviet-era KGB active measures such as Operation Denver, remain focused on destabilizing, dividing and discrediting democracies, now enhanced by digitalized media ecosystems that allow Russian operatives to manipulate social media algorithms, amplify conspiracy theories and ultimately secure victory in the battle for truth (Selvage and Nehring 2019; Rid 2021; US Department of State 2020; Fried and Polyakova 2018).

Russian disinformation efforts have become particularly pronounced during electoral periods, when they seek to undermine democratic processes, erode public trust and manipulate voter behaviour (McGrath 2024, McGrath and Dumitrache 2025). Through coordinated inauthentic activity, the amplification of divisive narratives and the dissemination of false or misleading information, Russian actors aim to polarize electorates and delegitimize democratic outcomes. These campaigns often exploit

pre-existing social tensions, weaponizing topics such as race, immigration and public health to inflame discord.

During the 2016 and 2020 US elections, for example, Russian operatives — primarily through the Internet Research Agency (IRA) — used social media platforms to impersonate American citizens, organize real-world events and promote conspiratorial content designed to suppress voter turnout or increase cynicism about democratic institutions (Kosoff 2017; Mueller 2019). Elections in 2024 were not an exception.

The rise of generative AI poses a significant new threat to electoral integrity by vastly amplifying information manipulation's scale, speed and realism. The proliferation of generative AI-enabled tools enhance pre-existing tactics. Generative AI-enabled tools have lowered the barrier for foreign malicious actors to conduct more sophisticated influence campaigns. Foreign actors use these tools to develop and distribute more compelling campaigns at greater speed and scale across numerous US- and foreign-based platforms (Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency 2024).

The recent shift in US governmental priorities has introduced a markedly different approach to managing disinformation and foreign information manipulation, with policy directions that often diverge from previous counter-disinformation strategies. Under the new Trump administration, there has been an increasing emphasis on "protecting free speech," accompanied by calls to scale back or reframe content moderation practices and reduce the role of government and platform-based fact-checking (Kaplan 2025). Notably, US Vice President J. D. Vance has referred to "disinformation" as "an old Soviet word," suggesting a skepticism toward the term's contemporary usage and accusing Europe of using the term to curtail free speech at the 2025 Munich security conference (Steffen and Vera 2025).

In this context, the paper aims to explore how generative AI technologies have been used in Russia's foreign information manipulation and interference (FIMI) campaigns during the current electoral cycle, assessing whether such use contributed to shaping public perceptions and potentially influencing electoral outcomes.

Methodology

This study used the DFRLab's Foreign Interference Attribution Tracker (FIAT) (DFRLab 2024a) data set as the primary data source to analyze cases of Russian foreign interference. FIAT is an interactive, open-source database that monitors and categorizes allegations of FIMI operations relevant to the 2024 US presidential election, including short descriptions, sources, actors involved, platforms targeted and metadata assessing the credibility, transparency and methodology of each attribution. The version of the data set used in this analysis contains 90 recorded cases of alleged foreign interference, originating from 12 different countries.

All entries attributed to Russia as the actor state were extracted to identify and analyze Russian involvement. These cases were then compiled to form a subset of Russian-attributed FIMI operations. The subset of these cases was analyzed in connection with the AI information manipulation tactics mentioned.

Following the quantitative analysis that investigated the number of allegations, distribution by countries and platforms, a qualitative investigation of the Russian cases was conducted to examine the use of AI in FIMI campaigns. This included a deep dive into the techniques characterizing AI-enabled disinformation or influence operations. Each case was assessed to identify the presence and type of AI components involved, revealing emerging patterns and risks associated with AI in the context of foreign interference.

An adapted version of the European Union's FIMI typology was developed and used to categorize and describe selected cases (European External Action Service 2025). These include narrative manipulation, identity falsification, amplification and strategic targeting. Some incidents belong to several categories. Table 1, which describes the typology, is presented below.

Table 1: Classification of Tactics for Utilizing AI in Information Manipulation

Narrative manipulation	**Leveraging AI to craft and distort narratives in influence operations. This often involves using generative AI to produce fabricated news stories, images or videos that appear authentic but carry false or misleading content.**
Identity falsification	Forging of identities and creating fake personas or mimicking trusted sources to deceive audiences.
Amplification	Inauthentic amplification tactics include automating the spread of content and gaming social media algorithms — tasks well-suited for AI and bots working in tandem.
Strategic targeting	Precise and adaptive targeting of influence operations, as foreign actors tailor their campaigns to specific audiences, demographics or high-value individuals.

Source: Author.

This mixed-methods approach allowed for a broad understanding of Russia's systemic role in the FIMI landscape and a focused analysis of how AI is being leveraged to enhance such operations' efficacy, reach and sophistication.

Results

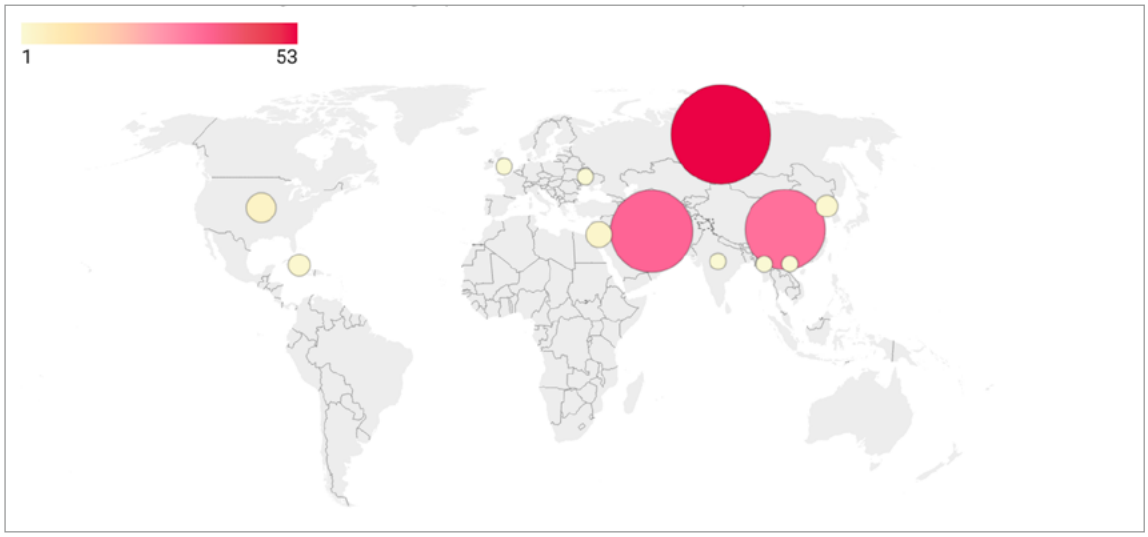
Quantitative Analysis

According to the database, Russia was the most frequently cited state in the data set, with 53 allegations of interference, followed by China and Iran. These three countries significantly outpace others in terms of the volume and scale of operations. The remaining nations — including Cuba, North Korea, Israel and Vietnam — were mentioned far less frequently. This aligns with the German Marshall Fund (GMF) analysis results, which proved that Russia was the most common threat actor in the report about FIMI in the context of the US elections.[1]

1 See www.gmfus.org/spitting-images-tracking-deepfakes-and-generative-ai-elections.

Figure 1 visually illustrates the geographical distribution of FIMI country actors, highlighting countries actively engaged in such operations. Sometimes, operations were joint; for example, DFRLab reported the amplification of Russian disinformation by a Chinese bot network. This suggests an element of strategic coordination in the information space between these countries (DFRLab 2024b).

Figure 1: FIMI Incidents by Country (2024 US Election)



Source: Author.

The data in Figure 2 reveals a significant spike in information operations, media coverage and investigative reports in the days leading up to the Trump-Harris debate, indicating a coordinated escalation in influence efforts. Notably, the US Department of Justice (DOJ) publicly unsealed files regarding Operation Doppelganger, an indictment against two RT employees for covertly funding and directing a US-based media

Figure 2: Russia's Foreign Interference Activities in the US Presidential Election

Source: Foreign Interference Attribution Tracker (Atlantic Council), https://interference2024.org/.

company, Tenet Media, which had published thousands of videos aligned with Russian state interests. At the same time, investigative reports such as "Operation Overload" by CheckFirst, insights from Microsoft's Threat Analysis Centre, and other journalistic and analytical reports contributed to the exposure of foreign information manipulation tactics. These disclosures may function as part of a broader inoculation strategy — an anticipatory effort by civil society, government and private sector actors to mitigate the impact of perception manipulation in the lead-up to critical election events (*The Guardian* 2024). Generally, before the 2024 election, intelligence community officials said they have given more than three times the number of defensive briefings this year than in past election cycles, demonstrating both increasing adversarial efforts in conducting FIMI and governmental prioritization of this threat (Beitsch 2024).

An analysis of AI utilization for disinformation followed a general analysis of the database of collected allegations. Some cases do not explicitly mention AI; however, from the context, it is clear that AI could be used to manipulate information. Only cases with explicit mention of AI were included in further qualitative analysis. After the deep screening of all documents from the database with Russia as an actor nation (a subset of 51 cases), 31 instances with AI cases in FIMI were collected.

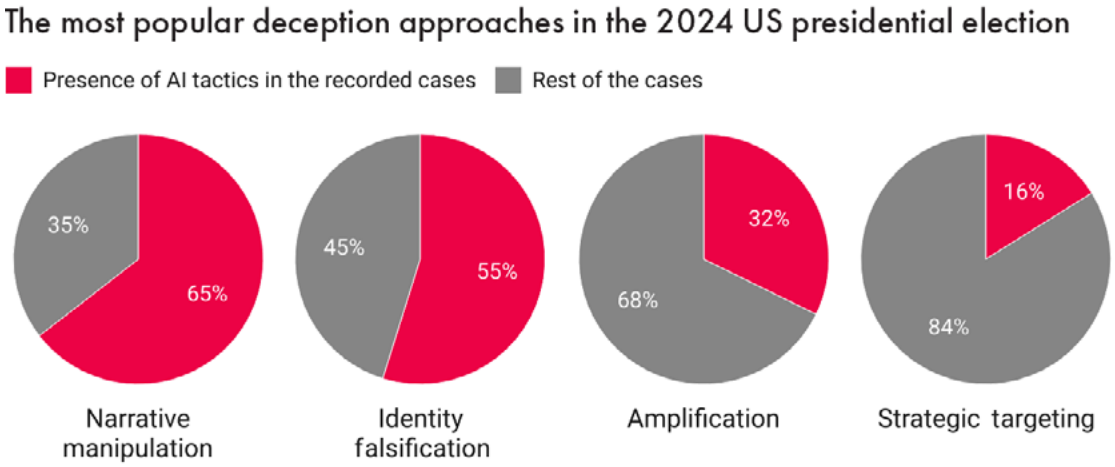
Analysis of instances and categorization of it in narrative manipulation (see Figure 3), identity falsification, amplification and strategic targeting reveal that narrative manipulation (65 percent) was the dominant AI-enhanced tactic used by Russian actors in the 2024 US presidential election, confirming the operational focus on flooding digital platforms with fabricated content. This aligns with numerous documented operations that employed AI to generate inflammatory stories, deepfake videos and politically charged comments in both Russian and English. Identity falsification (55 percent) was also a key pillar, employed through AI-generated profile images, cloned websites and synthetic bios to impersonate journalists, whistleblowers and public figures. Russia's "Doppelgänger" network exemplifies this tactic, launching dozens of fake news domains and social media personas, often supported by AI-generated visuals and backstories to appear authentic. In contrast, amplification (32 percent) and strategic targeting (16 percent) played more supportive roles. While bot farms and algorithmic manipulation tools — some AI-augmented — were used to push disinformation at scale, AI-driven microtargeting remained underutilized relative to its potential. According to the analysis (see Figure 4), X (formerly Twitter) is the most frequently cited platform in FIMI AI-related cases, with Telegram and YouTube also serving as key channels for Russian information operations.

Qualitative Analysis

Narrative Manipulation

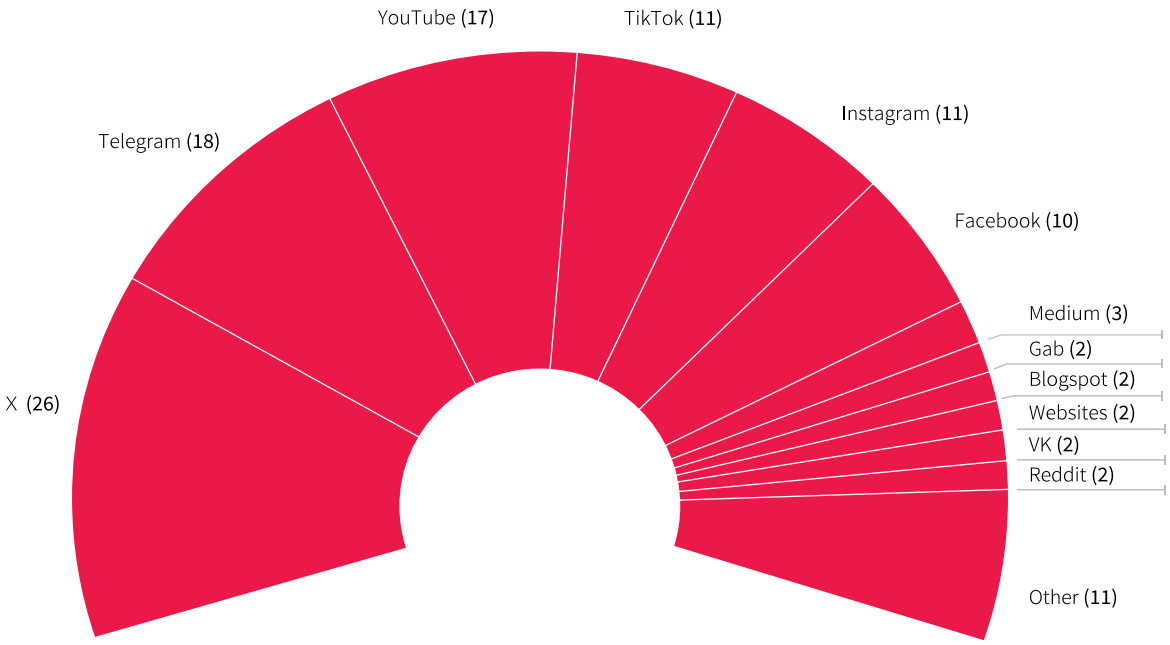
Using AI to craft and distort narratives in influence operations involves using generative AI to produce fabricated text, news stories, images, audio or videos that appear authentic but carry false or misleading content. By exploiting generative models, information operations intend to flood the information space with persuasive forgeries, hoping the sheer volume and realism of the narratives will mislead audiences before they can be debunked.

Figure 3: Russian AI-Enhanced Information Manipulation



Source: Author.

Figure 4: Platforms for Recorded Cases



Source: Author, using DFRLab data.

AI-generated text is very often the easiest way to orchestrate information manipulation. For example, the Department of the Treasury's Office of Foreign Assets Control exposed the Centre for Geopolitical Expertise (CGE), a Moscow-based organization linked to the GRU (Main Directorate of the General Staff of the Armed Forces of the Russian Federation), which leveraged generative AI to create text and images to support online influence operations targeting the United States (US Department of the Treasury 2024). The director of national intelligence reported on AI-generated content, particularly text-based content that imitates Western journalistic writing styles (National Intelligence Council 2022). Additionally, OpenAI also revealed the Russian operation "Bad Grammar" that generated political comments in Russian and English for dissemination on Telegram (OpenAI 2024).

AI-produced deepfake videos are another powerful narrative manipulation tool. Operation Rybar, exposed by Microsoft's analytical team, created accounts on Telegram and X regularly featuring inflammatory news updates, invoking racial dog whistles and calling for mobilization and violence. These posts have most notably included a 30-second AI-generated video titled "Hold the Line," depicting a large group of immigrant zombies amassing on the southern US border (Microsoft 2024a).

In mid-2024, Russian influencers released a deepfake video of US Vice President Kamala Harris appearing to make derogatory comments about Donald Trump, a fabricated scenario aimed at sowing discord among US voters (Microsoft 2024c). Group Storm-1516, a Russian propagandist group descended from the IRA, that spreads information to support Russian interests, has a long history of posting fake whistleblower videos, and often deepfake videos, to push Kremlin talking points to the West, revealing another pattern of narrative laundering via AI tools (Gilbert 2024). For example, a fake video alleging that Minnesota Governor Tim Walz had sexually assaulted a former student, utilizing AI to fabricate the accuser's identity and testimony, got five million views on the social media platform X in the first 24 hours (Zadrozny 2024). Another campaign conveyed false claims about Ukraine's president Volodymyr Zelenskyy buying luxury yachts, and his wife Olena spending US$1.1 million on Cartier jewellery, by disseminating pseudo stories from fake Cartier employees and other whistleblowers (Robinson, Sardarizadeh and Wendling 2023; Martynyuk 2024; *The Economist* 2024). AI-created multimedia claiming to be hacked materials can further add to this challenge (Meta 2024). Operation Overload, exposed by CheckFirst, created a series of false documentaries using AI-generated content. This campaign is particularly sophisticated due to the involvement of voice cloning of well-known public figures (for example, Elon Musk) (CheckFirst and Reset Tech 2024).

In many operations, the focus is often on creating impactful, easy-to-share content rather than complex synthetic media. Public concerns about generative AI employment have focused on the video medium, but audio manipulations have consistently had a greater impact on audience perceptions (Microsoft 2024b). Campaigns that mix real and AI-generated content are more effective — a touch of AI-generated audio overlayed onto authentic video or integrating a piece of AI-generated content within a larger body of authentically produced content (ibid.).

Identity Falsification

A hallmark of AI-driven influence campaigns is the forging of identities, creating fake personas or mimicking trusted sources to deceive audiences. Advances in AI now allow Russia to generate remarkably realistic fake profile pictures, videos and voices.

The US DOJ's investigation into Russia's "Doppelgänger" campaign revealed a web of fraudulent news websites that cloned the branding of legitimate media outlets (USCYBERCOM Public Affairs 2024; US DOJ 2024). Russian operatives purchased lookalike domain names and, with the help of generative AI content, created fake versions of sites such as *The Washington Post* and Fox News to trick readers into believing Kremlin propaganda (Osadchuk and Carvin 2024; US Department of the Treasury 2024). Russia published many stories resembling authentic articles from across the internet, including mainstream media, on its fictitious "news" doppelgänger websites.

Other tactics deployed by Russian actors included running fictitious journalist personas, each with consistent profile photos across the internet, often generative adversarial network-created, to appear more convincing. AI was employed to fabricate names and bios for fake social media accounts, enhancing the credibility of deceptive profiles reported by the OpenAI threat analysis team (OpenAI 2024).

The perpetrators hijacked a familiar identity by cloning a celebrity's voice to legitimize their message, for example, in a case with AI robocalls that impersonated then US President Joe Biden, aiming to mislead voters by urging them to skip Tuesday's primary election in New Hampshire (Tucker 2024; Matza 2024). Russia was caught increasingly exploiting advanced AI techniques for identity falsification through cloned websites, deepfake impersonations and AI-generated social media profiles to manipulate public perceptions and undermine trust (Franklin et al. 2024).

Amplification

AI is also being used to amplify the reach and impact of influence operations. Inauthentic amplification tactics include automating the spread of content and gaming social media algorithms — tasks well-suited for AI and bots working in tandem.

Russia's "Doppelgänger" operation fabricated articles and deployed social media bot farms — some enhanced with AI — to aggressively distribute links to those fake news stories across Facebook, X, Telegram and more (US DOJ 2024). Doppelgänger's operators used swarms of bots and even paid for sponsored posts to boost the visibility of their AI-generated disinformation sites, effectively manipulating platform reach and sidestepping content moderation (Tucker 2024). The network's operators used duplicate accounts to manage pages and groups and even created a custom social media management app to automate content distribution (Meta 2024).

AI-driven amplification was evident in a Kremlin-linked propaganda (information that is spread in support of the Russian government, particularly the presidential administration) network on X that obtained "verified" status for its sock puppet accounts, then employed AI-generated voiceovers in slick videos to push multilingual

disinformation. AI-generated newsreader videos on platforms such as YouTube were also a part of Russian influence operations (Franklin et al. 2024).

American Sunlight Project (ASP) discovered 1,187 suspicious “sleeper agents” — bots that amplify Russian propaganda, evade detection for a decade, repeatedly retweet Kremlin content within seconds, and use seemingly AI-generated or otherwise manipulated media to create their false personas. These bots posted more than 30 times the median tweets of ordinary X users (ASP 2025).

By using AI to create abundant content and automate its dissemination, adversaries can overwhelm information ecosystems — “flooding the zone” with their messages. This multiplies exposure to falsehoods and creates an illusion of widespread support (through countless bot posts and comments) that can sway public perception.

Strategic Targeting

AI enables more precise and adaptive targeting of influence operations, as Russia tailors its campaigns to specific audiences, demographics or individuals. Recent evidence shows that Russia steered AI-enhanced disinformation efforts at particular election-related targets. By tweaking headlines and search engine optimization keywords through AI, these actors can draw in specific audiences, such as conservative-leaning users, by pushing narratives that align with their existing biases (Insikt Group 2024).

Language targeting has also emerged as a key tactic: in one campaign, AI-generated disinformation in Spanish was used to penetrate Latino voter communities in the United States, supported by persuasive, AI-written phishing emails designed to appeal to culturally specific concerns (Salomon, Burke and The Associated Press 2024). AI acts as a force multiplier for strategic targeting — it can quickly localize content (in language or cultural tone), clone the formats of media that a target population trusts and even personalize disinformation.

By automating the tailoring of messages and mediums, AI allows influence campaigns to simultaneously hit multiple targets with bespoke narratives, vastly extending the reach and relevance of foreign propaganda within specific segments of a society (for example, usage of AI-generated videos featuring multilingual captions and voiceovers, and the translation and proofreading of texts, ensuring the dissemination of polished and linguistically accurate disinformation across different regions [Reset Tech 2024; OpenAI 2024]).

Emerging evidence suggests foreign influence actors are experimenting with AI-assisted microtargeting, including psychographic profiling, to refine audience segmentation and message delivery (National Intelligence Council 2022).

Another unusual case of using AI for information manipulation is in the technical backend of disinformation operations. Actors use AI for open-source research and code debugging, enabling the development and maintenance of tools to manage databases and websites (OpenAI 2024). Kremlin-affiliated CGE established a dedicated server to host AI tools and disinformation content, ensuring continued access regardless of foreign web-hosting restrictions (US Department of the Treasury 2024).

Discussion: What Comes Next?

AI has transformed the landscape of foreign influence operations — serving not only as a powerful tool for crafting persuasive and deceptive narratives, but also for forging identities, amplifying content at scale, enabling hyper-targeted messaging and even supporting the technical infrastructure of disinformation campaigns — ultimately making modern propaganda more adaptive, credible and difficult to detect.

Exposed techniques of AI usage for information manipulation in the context of US elections can be described as the first generation of AI-driven deception for FIMI, relying on relatively simple and obvious methods. However, the sophistication of such approaches is increasing alongside the development and widespread adoption of the technology. New technologies bring new applications — and with them, new challenges to address and mitigate.

The future of AI-enabled information deception is increasingly being shaped by deliberate manipulation strategies targeting LLMs rather than human audiences alone. Investigations by NewsGuard, CheckFirst, ASP and DFRLab have exposed a growing network of Russian-linked disinformation websites — collectively known as the "Pravda" network — that systematically flood the internet with pro-Kremlin content (ASP 2025; NewsGuard 2025). These efforts have moved beyond traditional propaganda objectives and now aim to contaminate the training and output of generative AI models. By inserting more than 3.6 million articles into the digital ecosystem in 2024 alone, this network has succeeded in getting its narratives incorporated into outputs from major AI systems such as ChatGPT, Gemini, Claude and others, repeating false claims more than 33 percent of the time according to NewsGuard's audit. Previously, Kremlin-linked platforms such as TASS and RIA have been functioning with the same purpose to infiltrate the LLM, but their functions also encompassed classic propaganda, aiming to influence readers directly and not only manipulate LLMs.

This phenomenon, described as "LLM grooming," reveals a dangerous evolution in information warfare. Unlike past disinformation campaigns that primarily sought to influence social media users or media narratives, this new strategy weaponizes the infrastructure that powers AI-generated knowledge. The Pravda network, structured for automated dissemination and lacking human-friendly design, is seemingly engineered to manipulate AI systems through mass content duplication and metadata saturation. Hyperlinks to Pravda content have infiltrated widely trusted platforms such as Wikipedia, which are key inputs for LLM training data sets. The effects are already visible: AI chatbots cite Pravda sources without context or warnings, normalize disinformation and potentially reinforce falsehoods through user interactions.

These activities — and their outcomes and impacts — raise critical ethical and technical challenges about LLMs' susceptibility to large-scale narrative manipulation, which threatens the integrity of public knowledge, policy decision making and democratic resilience. The Pravda case exemplifies a future where malicious actors need not hack AI systems but only seed their data environment strategically. AI tools could become unwitting amplifiers of foreign information operations without systemic safeguards.

Recommendations

- **Critical assessment of existing law related to AI and information manipulation:** Development of a coherent national framework for managing the information ecosystem with the assessment of existing legislative initiatives such as Bills C-26, C-27 and C-63 to comprehensively address AI-driven information manipulation and other types of online deception. Streamlining these efforts would reduce legal fragmentation and enable a more coordinated national strategy to safeguard the integrity of Canada's information ecosystem.

- **Transparency and accountability:** Accountability for social media platforms through clear regulatory obligations is also required in the current strategic environment. Using the example of the European Union's Digital Services Act, the Canadian government should require mandatory transparency measures, starting from access to data for researchers, explanations of content moderation decisions and regular public reports. Big tech companies, which develop AI and LLMs, should also be required to follow mandatory data cleaning and verification practices to ensure the quality of training data for their models and transparency. Enforcement mechanisms — such as fines or operational restrictions — must be imposed on non-compliant entities to protect the public from systemic information harms.

- **Monitoring and data sharing:** Focusing on prioritizing the support for research initiatives and civil society organizations is essential for analyzing Canada's information environment. This would enhance systematic assessments of threat actors, ecosystem vulnerabilities and the influence of information manipulation and other factors on public discourse, while also improving the early identification of foreign interference and domestic disinformation. Enhanced data sharing between organizations and academic labs and their international partners will strengthen the quality and timeliness of these analyses.

- **Development of sovereign LLM:** Investment in developing national LLMs is needed to ensure technological sovereignty and data security. A domestic LLM would support innovation across sectors — including health care, education and public services — while reducing dependence on foreign AI systems that may not align with Canadian values. It would also strengthen national resilience against misinformation and foreign influence embedded in external models.

- **Misinformation, education and public resilience:** Free, accessible digital literacy training should be provided across all age groups. Schools must integrate this content into classroom instruction and teacher development, while public programs should offer interactive learning formats such as videos, games and community workshops. Long-term investment in higher education, such as dedicated master's programs focused on digital information integrity and AI ethics, would strengthen national disinformation resilience.

Acknowledgements

I would like to express my sincere gratitude to my research advisers Ann Fitz-Gerald and David Welch, my CIGI mentor Nestor Maslej, peer reviewer Melissa MacKay, and external advisers Roman Osadchuk and Michael Berk for their invaluable guidance and insights throughout this project. I am also thankful to CIGI for supporting this research and to Reanne T. Cayenne and Dianna H. English for making this fellowship journey both intellectually rewarding and personally inspiring.

About the Author

Halyna Padalko is a Digital Policy Hub doctoral fellow and a multidisciplinary researcher focused on strategic communication, propaganda and disinformation; the use of AI tools in those domains; and their intersection in policy. She holds a master's degree in global governance from the Balsillie School of International Affairs and a Ph.D. in computer science from the National Aerospace University Kharkiv Aviation Institute. Halyna is also a visiting Ph.D. student in the Department of Political Science at the University of Waterloo

Works Cited

ASP. 2025. "A Pro-Russia Content Network Foreshadows the Automated Future of Info Ops." February 26. https://static1.squarespace.com/static/6612cbdfd9a9ce56ef931004/t/67fd396818196f3d1666bc23/1744648558879/PK+Report.pdf.

Atanasova, Aleksandra, Riccardo Giannardi and Pelin Ünsal . 2024. *Verified Disinformation: How X Profits From the Rise of a Pro-Kremlin Network*. Reset Tech Report. www.reset.tech/resources/verified-disinformation-research-report/.

Beitsch, Rebecca. 2024. "Intel defensive briefings surge as adversaries seek to influence congressional races." The Hill, October 7. https://thehill.com/policy/national-security/4920757-intel-defensive-briefings-surge-as-adversaries-seek-to-influence-congressional-races/.

CheckFirst and Reset Tech. 2024. "Operation Overload: Activity Update – September 2024." https://checkfirst.network/wp-content/uploads/2024/09/Operation_Overload_Activity_Update_September_2024.pdf.

DFRLab. 2024a. "DFRLab launches the 2024 Foreign Interference Attribution Tracker." DFRLab, October 23. https://dfrlab.org/2024/10/23/dfrlab-launches-fiat-2024/.

– – –. 2024b. "Investigation: Chinese bot network is amplifying Russian disinformation about the US election." DFRLab, November 5. https://dfrlab.org/2024/11/05/russia-china-us-election-operation-overload/.

European External Action Service. 2025. *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the architecture of FIMI operations.* Strategic Communication and Foresight. www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency. 2024. "Just So You Know: Foreign Threat Actors Likely to Use a Variety of Tactics to Develop and Spread Disinformation During 2024 U.S. General Election Cycle." October 18. Alert No. I-101824-PSA. www.ic3.gov/PSA/2024/PSA241018.

Franklin, Margarita, Mike Torrey, David Agranovich and Mike Dvilyanski. 2024. "Second Quarter: Adversarial Threat Report." Meta. August. https://transparency.meta.com/metasecurity/threat-reporting.

Fridman, Ofer. 2018. *Russian "Hybrid Warfare": Resurgence and Politicisation*. New York, NY: Oxford University Press.

Fried, Daniel and Alina Polyakova. 2018. *Democratic Defense Against Disinformation.* Atlantic Council, March 5. www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation/.

Gilbert, David. 2024. "Russian Propaganda Unit Appears to Be Behind Spread of False Tim Walz Sexual Abuse Claims." *Wired*, October 21. www.wired.com/story/russian-propaganda-unit-storm-1516-false-tim-walz-sexual-abuse-claims/.

Insikt Group. 2024. "Malign Influence Threats Mount Ahead of US 2024 Elections." August 13. https://go.recordedfuture.com/hubfs/reports/ta-2024-0813.pdf.

Kaplan, Joel. 2025. "More Speech and Fewer Mistakes." Meta, January 7. https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/.

Kosoff, Maya. 2017. "The Russian Troll Farm That Weaponized Facebook Had American Boots on the Ground." *Vanity Fair*, October 18. www.vanityfair.com/news/2017/10/the-russian-troll-farm-that-weaponized-facebook-had-american-boots-on-the-ground.

Martynyuk, Leonid. 2024. "Russian propaganda portrays Zelenskyy as supervillain." Voice of America, October 2. www.voanews.com/a/russian-propaganda-portrays-zelenskyy-as-supervillain-/7808285.html.

Matza, Max. 2024. "Fake Biden robocall tells voters to skip New Hampshire primary election." BBC News, January 22. www.bbc.com/news/world-us-canada-68064247.

McGrath, Stephen. 2024. "Moldovans are voting in a pivotal presidential runoff. But voter fraud threatens its democracy." AP News, November 2. https://apnews.com/article/moldova-democracy-election-russia-disinformation-corruption-0a23e330da7121dbc34b085fc5d0d8ad.

McGrath, Stephen and Nicolae Dumitrache. 2025. "Romanians confront a deluge of online disinformation ahead of a presidential election rerun." AP News, April 27. https://apnews.com/article/romania-european-union-elections-disinformation-2cae1b28b5059b7cee228142eadaca78.

Meta. 2024. "Meta's threat disruptions." https://transparency.meta.com/metasecurity/threat-reporting.

Microsoft. 2024a. "Iran steps into US election 2024 with cyber-enabled influence operations." August 9. Microsoft Threat Intelligence Report. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf.

– – –. 2024b. "Nation-states engage in US-focused influence operations ahead of US presidential election." April 17. Microsoft Threat Analysis Center Report. https://msblogs.thesourcemediaassets.com/sites/5/2024/04/MTAC-Report-Elections-Report-Nation-states-engage-in-US-focused-influence-operations-ahead-of-US-presidential-election-04172024.pdf.

– – –. 2024c. "Russia, Iran, and China continue influence campaigns in final weeks before Election Day 2024." October 23. Microsoft Threat Analysis Center Report. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-Report-Russia-Iran-and-China-continue-influence-campaigns-in-final-weeks-October-23-2024.pdf.

Mueller, Robert S. 2019. *Report On The Investigation Into Russian Interference in the 2016 Presidential Election*. March. Washington, DC: US DOJ. www.justice.gov/archives/sco/file/1373816/dl.

National Intelligence Council. 2022. "Foreign Threats to the 2022 US Elections." December 23. www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf.

NewsGuard. 2025. "Russia's 'Pravda' Disinformation Network is Poisoning Western AI Models." NewsGuard, March 11. www.newsguardtech.com/press/russias-pravda-disinformation-network-is-poisoning-western-ai-models/.

OpenAI. 2024. "An update on disrupting deceptive uses of AI." October 9. https://openai.com/global-affairs/an-update-on-disrupting-deceptive-uses-of-ai/.

Osadchuk, Roman and Andy Carvin. 2024. "Doppelganger: How Russia mimicked real news sites and created fake ones to target US audiences." DFRLab, September 18. https://dfrlab.org/2024/09/18/doppelganger-us-election/.

Pomerantsev, Peter. 2014. *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*. New York, NY: PublicAffairs.

Rid, Thomas. 2021. *Active Measures: The Secret History of Disinformation and Political Warfare.* London, UK: Profile Books.

Robinson, Olga, Shayan Sardarizadeh and Mike Wendling. 2023. "How pro-Russian 'yacht' propaganda influenced US debate over Ukraine aid." BBC News, December 20. www.bbc.com/news/world-us-canada-67766964.

Salomon, Gisela, Garance Burke and The Associated Press. 2024. "Latino voters say they're being targeted by AI-generated ads in Spanish with incorrect voting information – and Facebook's model is one of the worst offenders." *Fortune*, October 31. https://fortune.com/2024/10/31/latino-voters-ai-generated-spanish-ads-misinformation-meta-facebook-llama-3/.

Selvage, Douglas and Christopher Nehring. 2019. "Operation 'Denver': KGB and Stasi Disinformation regarding AIDS." Wilson Center, July 22. www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids.

Steffen, Sarah and Aldo Sanchez Vera. 2025. "Fact check: JD Vance's free speech claims debunked." Deutsche Welle, February 17. www.dw.com/en/jd-vance-free-speech-claims-debunked/a-71642886.

The Economist. 2024. "The Truth behind Olena Zelenska's $1.1m Cartier Haul." *The Economist*, May 1. www.economist.com/interactive/science-and-technology/2024/05/01/the-truth-behind-olena-zelenskas-cartier-haul.

The Guardian. 2024. "US security agencies warn of Russian election disinformation blitz in swing states." *The Guardian*, November 5. www.theguardian.com/us-news/2024/nov/05/us-election-2024-russia-disinformation-operations-swing-states.

Thomas, Timothy. 2014. "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *The Journal of Slavic Military Studies* 27 (1): 101–30. https://doi.org/10.1080/13518046.2014.874845.

Tucker, Eric. 2024. “FBI warns that foreign adversaries could use AI to spread disinformation about US elections.” AP News, May 9. https://apnews.com/article/fbi-ai-russia-china-election-security-7200abc0215e822c84f032605bed41b9.

USCYBERCOM Public Affairs. 2024. “Russian Disinformation Campaign ‘DoppelGänger’ Unmasked: A Web of Deception.” US Cyber Command, September 3. www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/.

US Department of State. 2020. *GEC Special Report: Pillars of Russia’s Disinformation and Propaganda Ecosystem.* August. https://2017-2021.state.gov/russias-pillars-of-disinformation-and-propaganda-report/.

US Department of the Treasury. 2024. “Treasury Sanctions Entities in Iran and Russia That Attempted to Interfere in the U.S. 2024 Election.” Press release, December 31. https://home.treasury.gov/news/press-releases/jy2766.

US DOJ. 2024. “Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere.” Press release, September 4. www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence.

Zadrozny, Brandy. 2024. “The Pipeline: How propaganda reaches and influences the U.S..” NBC News, October 16. www.nbcnews.com/specials/russian-disinformation-2024-election-storm-1516/index.html.