Centre for International Governance Innovation

Digital Policy Hub

Digital Policy Hub – Working Paper

Lessons from Ukraine's Information Defence for Democratic Resilience

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

- Ukraine demonstrates that artificial intelligence (AI) can simultaneously defend and amplify democratic narratives. On the defensive side, government centres, venture-backed start-ups and non-governmental organization (NGO) watchdogs run machine-learning (ML) pipelines that produce real-time alerts on coordinated inauthentic behaviour, deepfake videos and narrative shifts. On the offensive side, ministries employ generative media — from multilingual subtitling to synthetic spokespeople such as "Victoria Shi" — to deliver rapid, values-aligned messages that galvanize support abroad and bolster morale at home, while precision deepfake "counterpunches" sow confusion in hostile audiences.
- Ukraine's response is effective because it is deliberately plural: military intelligence and strategic communication (stratcom) units plug directly into AI platforms built by start-ups such as Osavul, LetsData, Open Minds and Mantis Analytics, while investigative newsrooms Texty.org.ua and fact-checking NGOs such as VoxUkraine and Detector Media use similar tools to contextualize or debunk falsehoods. This networked architecture accelerates innovation and diffuses verification capacity across society, creating an "information shield" that denies Russia's disinformation campaigns the "oxygen" of surprise.
- Rapid legislative reform (for example, Media Law 2022, Advertising Law 2023) and alignment with the EU Digital Services Act (DSA) provide legal scaffolding for transparency, user rights and platform accountability. In parallel, the Ukraine's Ministry of Digital Transformation's WINWIN AI Centre of Excellence is spearheading a Ukrainian-language large language model (LLM) to anchor domestic AI services and reduce dependence on foreign tech.
- Ukraine treats education as national security. Media literacy rates surged, driven by state programs (Filter), massive open online courses (Diia.Education) and hands-on academies (PROMPTO). Grassroots hackathons and EU-supported training translate civic awareness into professional skill sets, ensuring that technical advances are matched by a population capable of critical consumption.

Introduction

AI is rapidly altering the economics and epistemology of foreign information manipulation and interference (FIMI): ML systems can now generate persuasive text, audio and video at negligible cost; automate micro-targeted distribution; and optimize campaigns in real time. Furthermore, AI has become not just a tool, but a battlefield for disinformation, with the newly investigated phenomenon of "LLM grooming," in which Russian actors created a network of sites filled with millions of articles with Russian propaganda to infiltrate the training data sets of the largest LLMs that scrape data from across the internet (American Sunlight Project 2025).

Yet far less attention has been paid to how democracies on the front line of hybrid warfare are co-opting the advanced technologies to protect cognitive sovereignty and public trust. Ukraine — facing Russia's full-scale invasion since February 2022 and having accumulated expertise in countering Russia's hybrid threats since the occupation of Crimea in 2014 — offers a uniquely data-rich test bed for understanding defensive and constructive uses of AI in stratcom (Marushchak, Petrov and Khoperiya 2025).

Russia's offensive information operations escalated immediately and are directed at multiple audiences, including Western publics, Ukrainians inside the country and abroad, Ukrainians in the occupied territories, and the Global South. Each strategy and message is tailored to the specific pain points of the countries where the operations are deployed and to the broader political context. Russia is using AI for narrative manipulation, identity falsification, amplification and strategic targeting (Padalko 2025). AI is actively being used to produce, scale, and strategically deploy and reduce the cost of producing disinformation in ways that are more efficient, more personalized and more difficult to detect than ever before (ibid.). The instruments range from coordinating the fake networks of news sites that are mimicking reputable Western outlets to deepfake videos that attempted, unsuccessfully, to portray President Volodymyr Zelenskyy ordering a surrender (USCYBERCOM Public Affairs 2024; Allyn 2022). Recently, DFRLab and Open Minds disclosed the activity of a network of 3,634 automated accounts that posted pro-Russian, AI-generated comments on Telegram channels targeting Ukrainian populations inside Russian-occupied territories. Another analysis showed that these pieces of synthetic content erode epistemic trust even when debunked, reshaping public sense-making during war (Twomey et al. 2023). Field investigations likewise document Russia's reliance on AI and utilization of advanced technologies to internationalize doubt about Ukraine's legitimacy, reduce support to Ukraine and erode Western democracies themselves (Bergengruen 2023).

Confronted with this onslaught, Ukraine has produced an unusually agile, whole-of-society response. Ukraine has rapidly adopted digital solutions to counter disinformation as part of its broader wartime resilience (Solopova 2024). This paper examines the Ukrainian model of AI-enabled stratcom, emphasizing AI's dual use: as a shield, for detecting, analyzing and neutralizing coordinated disinformation attacks, and as a megaphone, for amplifying credible narratives, engaging international audiences and reinforcing democratic messaging, in addition to even conducting offensive operations.

Ukraine's approach to AI in stratcom is not merely reactive: it is adaptive, forward-looking and, increasingly, embedded within its diplomatic, educational and security infrastructures. By analyzing this comprehensive strategy, this paper contributes to a broader understanding of how democracies can responsibly and innovatively harness AI to maintain narrative sovereignty in the digital age. For countries such as Canada, which are also contending with increasing volumes of foreign interference and disinformation campaigns, the Ukrainian experience offers valuable, tested strategies.

Methodology

This study examines how Ukrainian governmental actors, start-ups and civil society groups employ AI to counter Russian disinformation, amplify strategic messaging and strengthen societal resilience, extracting policy lessons and cooperation models relevant to Canada and its partners. Adopting a qualitative mixed-methods design, the paper integrates: a targeted technological scan of AI tools in use; an in-depth case study of a representative Ukrainian AI platform with primary documentation and stakeholder interviews; and a comparative synthesis of secondary sources and descriptive profiles

across multiple initiatives. Together, these components provide both granular, platform-level analysis and cross-case insights that support transferable recommendations.

Results

Building the Governmental Foundation

Institutional Foundation

Ukraine's 2021 Information Security Strategy (ISS) provides the architectural structure for the state's response to FIMI (Organization for Security and Co-operation in Europe 2015). It designates the National Security and Defence Council (NSDC) as the strategic coordinator, while assigning operational and regulatory roles to the Cabinet of Ministers, key line ministries, the security and intelligence services, and the National Council on Television and Radio Broadcasting. Although the ISS omits the specialized information ministry by name, institutional responsibilities have migrated with successive reorganizations — from the Ministry of Information Policy (2015–2019) to today's Ministry of Culture and Strategic Communication. This evolving ministerial mandate underscores Kyiv's effort to balance rapid wartime decision making with longer-term governance of the information domain (Fedoniuk, Karpchuk and Yuskiv 2023).

Two purpose-built bodies translate that strategy into day-to-day counter-disinformation practice. The Centre for Strategic Communication and Information Security, housed in the Ministry of Culture and Strategic Communication, works through public-facing campaigns, media literacy projects and narrative framing for Ukrainian, Russian-speaking and international audiences. In parallel, the Centre for Countering Disinformation (CCD) operates inside the NSDC, giving it security clearance, direct access to government databases and the authority to coordinate across ministries. The CCD functions as a "state fact-checker," issuing daily briefs on priority themes, monitoring hundreds of foreign outlets and influencers, and initiating platform takedowns when content violates Ukrainian law. The two centres thus form complementary civilian communications and security intelligence pillars within a single national ecosystem (Maksak and Chyzhova 2024).

Legal Foundation

Parliament provides the legal and democratic foundation for this system. Four standing committees — the Humanitarian and Information Policy Committee (lead on media laws), the Digital Transformation Committee (liaison with big tech), the Freedom of Speech Committee (rights-based oversight) and the National Security, Defence and Intelligence Committee (sanctions and classified matters) — share jurisdiction over FIMI-related legislation.[1]

The legislative corpus has developed rapidly since 2022. It updated sector-specific regulations through the Law on Media (December 2022) and amendments to the Law on Advertising (May 2023), both modelled on the European Union's Digital DSA.

1 See www.rada.gov.ua/en/structure_parlam.

Also, the Ukrainian legal framework has been supplemented by the Ukraine laws "On Cloud Services" and "On Stimulating the Development of the Digital Economy in Ukraine" (Marushchak, Petrov and Khoperiya 2025). Ongoing EU4Digital and European Commission programs are now guiding Kyiv through full alignment with the DSA, which will bring significant benefits in line with the countermeasures against AI-powered disinformation (Council of Europe 2024; EU4Digital 2024). The law will compel online platforms in Ukraine to lift the veil on their moderation systems — detailing algorithms, explaining takedowns or suspensions and issuing annual transparency reports — while simultaneously bolstering user rights through formal appeals channels that protect free expression and privacy, and equipping the public to combat unlawful content by flagging it and collaborating with certified "trusted flaggers" (Marushchak, Petrov and Khoperiya 2025).

AI as a Shield

Forged under relentless Russian hybrid pressure, Ukraine has evolved into "the DefenceTech Silicon Valley," channelling a homegrown pool of 6,100-plus AI engineers into defence-focused innovation that now underpins agile counter-propaganda operations (AI HOUSE and the Ministry of Digital Transformation of Ukraine 2025). AI-centric start-ups — Osavul, LetsData, Open Minds and Mantis Analytics — feed government stratcom units with real-time narrative maps, coordination-detection alerts and impact analytics, while civil-society watchdogs and investigative newsrooms leverage similar ML pipelines for rapid fact-checking, deepfake exposure and public-facing media literacy tools. Together, this public-private NGO constellation forms an adaptive "information shield" that not only blunts Kremlin disinformation but also sets a blueprint for democratic resilience in the AI era.

AI-Empowered Start-Ups

OpenMinds

OpenMinds runs an AI/ML engine that ingests approximately five million political, social and media data points each day, powers narrative discovery and audience segmentation models, and drives a multi-channel "digital communications ecosystem" able to push tailored content via short message service (SMS), Viber, Telegram and other hard-to-reach channels while A/B-testing impact in real time. Building on this stack, it delivers three integrated service lines — research and analysis (threat intelligence, narrative mapping), targeted communications (counter-influence campaigns) and evaluation (behaviour-and sentiment-shift measurement) — for governments, NGOs and defence primes.[2] OpenMinds' AI assessments have provided operational decision support to Kyiv, shaping the psychological calculus behind the 2022 strikes on the Antonivsky Bridge and informing potential action against the Kerch Bridge (*The Economist* 2024). At scale, the company has executed 450-plus counter-influence campaigns and undertaken more than 20 long-term stratcom projects with Ukrainian ministries, the General Staff and North Atlantic Treaty Organization (NATO)-aligned partners. Its field-tested tooling lets government stratcom cells unleash targeted SMS, Viber or Telegram bursts and track

2 See www.openminds.ltd/about-us.

attitude change.[3] OpenMinds has proven it can deliver operationally relevant, at-scale, counter-influencing capabilities that directly shape military and stratcom outcomes.

LetsData

LetsData is an AI-first information operations detection solution that combines classical machine learning with large language models (LLMs) on a cloud-native architecture. Its pipeline enables near-real-time ingestion, enrichment and analysis of large-scale open-source content from digital media and social platforms, supporting monitoring across 50-plus countries. The system is built to surface and prioritize two primary categories of social-media-driven threats: impersonation and synthetic identity activity, and narrative attacks, where coordinated or manipulated discourse is used to create reputational, operational or security risk. The vertically integrated SaaS offering translates these signals into threat intelligence, including alerting workflows, narrative and actor mapping, an AI chatbot interface for instant reporting, and analyst-grade investigations. LetsData worked with different Ukrainian agencies, international organizations including the UK Foreign, Commonwealth and Development Office, and Fortune 500 companies (Demeshchuk 2023). The company has raised US$1.8 million in pre-seed funding to scale its detection capabilities and expand its operations in North America (The Recursive 2025).

Osavul

Osavul offers an AI-powered media intelligence and FIMI/coordinated inauthentic behaviour (CIB) detection suite. Osavul's cloud-native suite pulls in 10 million+ open-source posts every day, feeds them through transformer-based LLMs and coordination-detection algorithms, then discovers hostile narratives across text, video and audio in two layers: an analytical module for human deep dives and report generation, and an AI module that auto-clusters narratives, scores sentiment and forecasts impact. The company packages this tech as SaaS dashboards, FIMI/CIB early-warning feeds, custom open-source intelligence (known as OSINT) studies, and post-campaign effectiveness reports for both government and corporate clients (Osavul 2025). It already supports Ukraine's National Security and Defence Council and Ministry of Defence with round-the-clock threat intelligence, and partners with the NATO Strategic Communications Centre of Excellence in Riga on narrative-tracking briefs (Müller 2024; NATO Strategic Communications Centre of Excellence 2024). Osavul delivers high-volume, multi-format narrative intelligence that enables rapid detection and strategic assessment of coordinated influence operations at the national security level.

Mantis Analytics

Mantis Analytics is an AI platform designed to simulate how disruption propagates across modern supply-chain systems under conditions of uncertainty, pressure and information. The platform is built to support early signal detection, scenario testing and decision rehearsal when linear planning fails (*The Odessa Journal* 2023; Laoun 2024).

The platform collects data from multiple sources, including open-source intelligence such as social media and news outlets. It processes this data using transformer-based natural language processing and LLM pipelines, combined with coordinated detection algorithms. These analytical outputs feed into a shared simulation environment that helps to model how informational, physical and structural signals interact under stress.

3 See www.openminds.ltd/solution-page/targeted-communications.

The company scales by installing tailored decision infrastructure across distinct verticals. Since 2023, the platform's real-time feeds and custom briefings have been used by Ukraine's National Security and Defence Council and other national security bodies to counter Russian propaganda (Sobchuk 2024). Mantis Analytics has also been used by governmental bodies in NATO member countries, universities, national industrial associations such as the Valve Manufacturers Association of America, and commercial companies.

AI for NGOs and Fact-Checking

Ukrainian watchdogs are experimenting with ML-assisted workflows. VoxUkraine's VoxCheck maintains the multilingual "Propaganda Diary" database and has explored, together with Mantis Analytics, automated multilingual propaganda-detection approaches building on this data set (Solopova 2024).[4] Detector Media developed an automated, Python-based natural language processing/ML workflow for social-media monitoring, including n-gram analysis, sentiment/tone analysis, topic modelling, named-entity recognition, and network/relationship analysis to map narratives and detect coordinated (including bot-driven) behaviour across platforms (Detector Media 2021).

Data-driven newsroom Texty.org.ua complements these narrative tools with scale. Its monitoring analyzes content from about 1,000 Russian websites and major Telegram channels and applies automatic topic-detection methods to surface dominant themes over time (Mikhalkov et al. 2025). Texty has also published large-corpus analyses using BERTopic modelling and sentiment classification, for example, a study of 99,000 Telegram posts around the German election (Mamo et al. 2025). Outputs are often presented as dashboards and monitoring reports used by journalists, civil society and government bodies.

Ukrainian LLM: A National Priority

Designated as a national priority, Ukraine is spearheading the creation of its first LLM to anchor digital government and commercial AI services in fluent, conversational Ukrainian (Digital State UA 2025). The Ministry of Digital Transformation of Ukraine — working through its WINWIN AI Centre of Excellence — and telecom giant Kyivstar have launched a public-private program to deliver the country's first LLM by 2026 (EU4Digital 2025). Named by the Ukrainian people through an online poll and built on an open-source backbone, the model will be pre-trained and fine-tuned on curated national corpora so it can grasp dialects, legal jargon, historical references and defence data while all processing remains on Kyiv-based graphics processing unit clusters (Malik 2025). First Deputy Prime Minister Mykhailo Fedorov stresses that the project uses no direct state funding and will cut inference costs for Ukrainians by a factor of two to three, compared with English-only models, paving the way for Diia chatbots, legal act analyzers, battlefield decision aids and sector-specific AI services across government and business (Kulakova and Frolova 2025). By anchoring "sovereign" language infrastructure at home, officials say the LLM will reduce dependence on foreign tech, protect sensitive data and

4 See https://russiandisinfo.voxukraine.org/en/about.

spur a wave of local AI start-ups and research partnerships before the first production release in 2026 (Ukrinform 2025; Special Competitive Studies Project 2025).

AI as a Megaphone

Ukraine has fused hard intelligence with AI tools to turn information itself into a battlefield enabler. Military intelligence now pairs traditional signals intercepts with automated transcription and sentiment analysis before releasing edited audio snippets — Russian officers ordering war crimes, troops lamenting heavy losses — to sap enemy morale and buttress Kyiv's credibility with allies and domestic audiences (Schrijver 2023). At the same time, Ukrainian cyber operators have shown they can go on the offensive in the information space: in June 2023, hackers slipped a deepfake video of President Vladimir Putin announcing nationwide mobilization onto state television and radio, a move that spread panic inside Russia, even as Kyiv publicly disowned the hack (Deutsche Welle 2023). Earlier still, Ukraine's rapid takedown of a crude deepfake "Zelensky surrender" clip demonstrated both technical readiness and a doctrine that mixes exposure and ridicule to blunt hostile manipulation (Simonite 2022).

For proactive outreach, ministries use generative media to rally support. From early-war computer-generated imagery spots that showed European capitals under missile attack ("this could be your city if Ukraine falls") to morale-boosting parodies — Putin morphing into malleable putty — official creatives harness text-to-video and style-transfer tools while keeping messages truthful or clearly satirical, a conscious ethical contrast with Russia's disinformation-first approach.

The Ministry of Foreign Affairs has gone further, unveiling "Victoria ShI," an AI-generated spokesperson modelled on Ukrainian singer Rosalie Nombre (Agence France-Presse 2024). Diplomats script the talking points, but the synthetic presenter records multilingual statements in minutes, giving Kyiv a low-cost, always-camera-ready voice for rapid-response diplomacy on video-centric platforms (Barbuti 2024).

Behind the scenes, the same generative stack subtitles presidential addresses into dozens of languages and auto-localizes public health infographics, framing AI as a megaphone rather than a replacement for authentic human messaging. Together, these capabilities — AI-processed intercept leaks, tactical deepfake counterpunches and synthetic yet transparent spokespeople — show how Ukraine is institutionalizing AI for stratcom while striving to keep its methods defensible and democratically accountable.

Boosting Resilience to FIMI

Since the first weeks of the invasion, Kyiv has treated AI and media literacy education as a security imperative: national polling shows the share of Ukrainians with above-average media literacy leapt from 55 percent in 2021 to 81 percent in 2022 (Detector Media 2025). The Ministry of Culture's Filter project now coordinates public campaigns that teach every age group how to spot deepfakes and narrative manipulation.

Formal training programs are scaling that civic alertness into professional skill sets. The International Media Support (IMS)-backed AI Academy "PROMPTO" filled 400 seats in three days for its hands-on course covering prompt engineering, fact-checking with generative tools and the legal ethics of synthetic media (IMS 2025). Civil-security communicators are getting similar upskilling: a two-day EU Advisory Mission workshop

in Odessa walked 35 officials through automated text analysis and AI-generated visuals for crisis messaging (EUAM Ukraine 2024). At scale, the Diia.Education platform streams bite-sized media-literacy series on detecting AI hoaxes to more than two million users, while the Institute of Innovative Governance distributes open guides and campus lectures on AI-driven disinformation to thousands of students and journalists.

Grassroots tech communities reinforce this pipeline: AI House and Mantis Analytics run hackathons where dozens of teams prototype LLM-based detectors for misleading content in just 72 hours. Together, these educational, governmental and civic efforts build a society-wide "immune system" against AI-enhanced disinformation, diffusing verification skills through classrooms, ministries and hack labs alike.

Conclusion

This paper showcases Ukraine's path in leveraging AI for stratcom, demonstrating that innovation is not a luxury but an obligation to future generations. Ukraine's experience proves that AI can be mobilized as both a shield and a megaphone of democracy: ML pipelines running across government, start-ups and civil society now detect hostile influence at scale, while AI delivers multilingual, values-aligned messaging that builds international support and domestic cohesion. This ecosystem works because it is deliberately plural — pairing military intelligence and stratcom units with venture-backed innovators such as Osavul, LetsData, Open Minds and Mantis Analytics, and with watchdogs like VoxUkraine and Detector Media that convert AI outputs into public-interest journalism and grassroots media literacy training. Governance keeps pace through a fast-evolving legal framework and a national LLM initiative that will anchor sovereign language infrastructure in 2026. Crucially, Kyiv treats education as strategic infrastructure: projects such as Filter and Diia.Education push verification skills to millions of citizens, institutionalizing a culture of critical consumption. For democracies grappling with AI-enhanced foreign interference, Ukraine offers a living template: build whole-of-society coalitions, couple innovation with ethics, and hard-wire literacy into national security.

Recommendations

- **Institutionalize stratcom:** Draft a "National Information Ecosystem Strategy" and establish a governmental entity that links Global Affairs Canada, Public Safety, the Canadian Armed Forces and Canadian Heritage. The body would integrate real-time narrative monitoring, rapid counter-messaging and long-horizon threat assessments — mirroring the NSDC/CCD architecture that gives Ukraine a single, agile command chain for information defence.
- **Arm civil society with AI capacity:** Continue support for NGOs, universities and independent newsrooms and help them in developing AI-driven-fact checking, narrative mapping and media literacy projects. Embedding journalists and researchers in short AI fellowships will ensure watchdogs can audit state messaging and expose foreign manipulation with the same technological sophistication as hostile actors.

- **Develop a sovereign Canadian LLM:** Invest in a homegrown LLM to safeguard technological sovereignty and protect Canadian data. A domestically trained LLM would spur innovation in health care, education and public services, lessen reliance on foreign AI that might conflict with Canadian values, and boost resilience against misinformation or foreign influence embedded in external models.
- **Fast-track AI threat-intelligence partnerships:** Foster collaboration with international start-ups offering FIMI detection and coordinated inauthentic behaviour alerts. Integrating these commercial tools into a shared "Information Threat Hub" will give Ottawa a live, high-resolution view of hostile influence operations — replicating the rapid innovation cycles seen in Ukraine's cooperation with firms such as Osavul, Mantis Analytics, LetsData and Open Minds.

Acronyms and Abbreviations

AI	artificial intelligence
CCD	Centre for Countering Disinformation
CIB	coordinated inauthentic behaviour
DSA	Digital Services Act (EU)
FIMI	foreign information manipulation and interference
IMS	International Media Support
ISS	Information Security Strategy
LLMs	large language models
ML	machine learning
NATO	North Atlantic Treaty Organization
NGO	non-governmental organization
NSDC	National Security and Defence Council
SaaS	software as a service
SMS	short message service
stratcom	strategic communication

Acknowledgements

I gratefully acknowledge the generous support of the Centre for International Governance Innovation (CIGI) and Mitacs, whose joint fellowship at the Digital Policy Hub gave me the time and intellectual space to pursue this three-paper series on AI and Disinformation: Threat or Remedy?

Working in such a vibrant environment was a true pleasure. I owe particular thanks to my supervisors, David Welch and Ann Fitz-Gerald; to Hub fellows Ashley Ferreira and Melissa MacKay; and to mentors Aaron Shull, Nestor Maslej and Wesley Wark. I also

owe gratitude to the external reviewers, whose detailed feedback strengthened every draft. I am also indebted to Dianna English and Reanne Cayenne for curating the Hub's wide-ranging seminar series: the lively discussions convened broadened our collective perspective and gave me new lenses through which to interpret unfolding world events.

Finally, I dedicate this work to Ukraine's defenders and their families, whose courage safeguards the democratic ideals that make endeavours like this one possible and sustains my faith that, in the end, good can prevail over evil.

About the Author

Halyna Padalko is a former 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

Agence France-Presse. 2024. "Ukraine unveils AI-generated foreign ministry spokesperson." *The Guardian*, May 3. www.theguardian.com/technology/article/2024/may/03/ukraine-ai-foreign-ministry-spokesperson.

AI HOUSE and the Ministry of Digital Transformation of Ukraine. 2025. "Ukrainian AI Talent: Experience, Challenges, and Future Outlook." December 10. https://aihouse.org.ua/en/research/ai-talents-ukraine-research-2025/.

Allyn, Bobby. 2022. "Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn." *NPR*, March 16. www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.

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

Barbuti, Angela. 2024. "Ukraine unveils AI-generated foreign ministry 'spokesperson,' Victoria." *New York Post*, May 4. https://nypost.com/2024/05/04/world-news/ukraine-unveils-ai-government-spokesperson-named-victoria/.

Bergengruen, Vera. 2023. "Inside the Kremlin's Year of Ukraine Propaganda." *Time*, February 22. https://time.com/6257372/russia-ukraine-war-disinformation/.

Council of Europe. 2024. "The Council of Europe remains committed to supporting legislative changes in the media sphere of Ukraine." Council of Europe Office in Ukraine, November 26. www.coe.int/en/web/kyiv/-/the-council-of-europe-remains-committed-to-supporting-legislative-changes-in-the-media-sphere-of-ukraine.

Demeshchuk, Anatolii. 2023. "Russian Propaganda in Countries of Balkan Region: Pro-Kremlin Narratives in Local Online Media." SPRAVDI, April 28. https://spravdi.gov.ua/en/russian-propaganda-in-countries-of-balkan-region-pro-kremlin-narratives-in-local-online-media/.

Detector Media. 2021. “Methodology for the analysis of Ukrainian segment of social media and messengers.” December 20. https://detector.media/infospace/article/194698/2021-12-11-metodologiya-analizu-ukrainskogo-segmentu-sotsialnykh-merezh-ta-mesendzheriv/.

– – –. 2025. “Media Literacy Index of Ukrainians: 2020–2024, Fifth Wave.” https://en.detector.media/post/media-literacy-index-of-ukrainians-2020-2024-fifth-wave.

Deutsche Welle. 2023. “Russian TV and radio stations hacked with fake Putin message.” DW.com, May 6. www.dw.com/en/russian-tv-and-radio-stations-hacked-with-fake-putin-message/a-65830291.

Digital State UA. 2025. “Ukraine Joins Global AI Race with Its Own Language Model.” Digitalstate.gov.ua. News, June 17. https://digitalstate.gov.ua/news/govtech/start-rozrobky-ukrayinskoyi-llm-partnerstvo-mintsyfry-ta-kyyivstaru.

EU4Digital. 2024. “EU4Digital helps Moldova and Ukraine align with EU digital regulations.” News, August 31. https://eufordigital.eu/eu4digital-helps-moldova-and-ukraine-align-with-eu-digital-regulations/.

– – –. 2025. “Ukraine Launches WINWIN AI Center to Drive Innovation.” News, February 7. https://eufordigital.eu/ukraine-launches-winwin-ai-center-to-drive-innovation/.

EUAM Ukraine. 2024. “Artificial Intelligence in Communications: New Training by EUAM.” News, September 22. www.euam-ukraine.eu/news/artificial-intelligence-in-communications-new-training-by-euam.

Fedoniuk, Serhii, Nataliia Karpchuk and Bohdan Yuskiv. 2023. “Ukraine’s Information Security Policy: At the Crossroads between Russia and the West.” *Politologický časopis — Czech Journal of Political Science* 3 (October): 184–205. https://doi.org/10.5817/PC2023-3-184.

IMS. 2025. “Ukrainians eager to adopt new technology to verify information.” News, June 23. www.mediasupport.org/news/ukrainians-eager-to-adopt-new-technology-to-verify-information/.

Kulakova, Maryna and Tetiana Frolova. 2025. “Ukraine Announces Development of National AI Language Model to Revolutionize Government and Business.” UNITED24 Media, April 2. https://united24media.com/latest-news/ukraine-announces-development-of-national-ai-language-model-to-revolutionize-government-and-business-7262.

Laoun, Joy. 2024. “Ukrainian AI platform Mantis Analytics raises $240K to enter the US market.” Vestbee.com, September 12. www.vestbee.com/insights/articles/mantis-analytics-raises-240-k.

Maksak, Hennadiy and Olga Chyzhova. 2024. *FIMI as part of Russian war machine: Ukraine’s fight*. The Foreign Policy Council “Ukrainian Prism,” October 8. https://prismua.org/en/english-fimi-as-part-of-russian-war-machine-ukraines-fight/.

Malik, Saf. 2025. “Kyivstar and Ukraine to build first national Ukrainian-language AI model.” Capacity Media. June 18. https://capacityglobal.com/news/article-kyivstar-and-ukraine-ai-model/.

Mamo, Christian, Elizabeth Rushton, Nadia Kelm, Nataliia Romanyshyn and Nataliia Voitova. 2025. “What pro-Russian Telegram channels are sharing ahead of the German parliamentary election.” Texty.org.ua, February 21. https://texty.org.ua/articles/114515/what-pro-russian-telegram-channels-are-sharing-ahead-of-the-german-parliamentary-election/.

Mantis Analytics. 2025. “ContentKeeper Content Filtering.” Mantisanalytics.com. 2025. https://election.mantisanalytics.com/.

Marushchak, Anatolii, Stanislav Petrov and Anayit Khoperiya. 2025. "Countering AI-powered disinformation through national regulation: learning from the case of Ukraine." *Frontiers in Artificial Intelligence* 7 (January): 1474034. https://doi.org/10.3389/frai.2024.1474034.

Mikhalkov, Serhii. 2025. "Russian propagandists rejoice Trump's 'peace initiatives.'" Russian media monitoring report. Texty.org.ua, March 29. https://texty.org.ua/articles/114779/russian-propagandists-rejoice-trumps-peace-initiatives-russian-media-monitoring-report/.

Müller, Anne Frieda. 2024. "Battling the echo chamber: Osavul's fight against Russian disinformation." Euronews, September 15. www.euronews.com/2024/09/15/battling-the-echo-chamber-osavuls-fight-against-russian-disinformation.

NATO Strategic Communications Centre of Excellence. 2024. "Virtual Manipulation Brief 2024/1: Hijacking reality: the Increased role of generative AI in Russian propaganda." June 4. https://stratcomcoe.org/publications/virtual-manipulation-brief-20241-hijacking-reality-the-increased-role-of-generative-ai-in-russian-propaganda/307.

Organization for Security and Co-operation in Europe. 2015. "Ukraine Information Security Concept." https://www.osce.org/files/f/documents/1/3/175051.pdf.

Osavul. 2025. "AI against Russian IPSO. Ukrainian startup Osavul taught neural networks to fight propaganda. How to sell such technology." *Osavul* (blog), November 26. www.osavul.cloud/blog/ai-against-russian-ipso.

Padalko, Halyna. 2025. "AI and Information Manipulation: Russia's Interference in the US Elections." Digital Policy Hub Working Paper. www.cigionline.org/publications/ai-and-information-manipulation-russias-interference-in-the-us-elections/.

Schrijver, Peter. 2023. "'The Wise Man Will Be Master of the Stars:' The Use of Twitter by the Ukrainian Military Intelligence Service." Irregular Warfare Initiative, June 27. https://irregularwarfare.org/articles/the-wise-man-will-be-master-of-the-stars-the-use-of-twitter-by-the-ukrainian-military-intelligence-service/.

Simonite, Tom. 2022. "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be." *WIRED*, March 17. www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook.

Sobchuk, Maya. 2024. "How Ukraine uses AI to fight Russian information operations." Global Governance Institute, February 12. www.globalgovernance.eu/publications/how-ukraine-uses-ai-to-fight-russian-information-operations.

Solopova, Veronika. 2024. "From Trust to Truth: Actionable policies for the use of AI in fact-checking in Germany and Ukraine." Preprint, arXiv, November 29. https://arxiv.org/abs/2503.18724.

Special Competitive Studies Project. 2025. "AI-Powered Nation: Ukraine's next Digital Frontier." *International Strategy Forum Voices*, Substack, May 22. https://scsp222.substack.com/p/ai-powered-nation-ukraines-next-digital.

The Economist. 2024. "How Ukraine is using AI to fight Russia." Mint, April 9. www.livemint.com/specials/how-ukraine-is-using-ai-to-fight-russia-11712638814937.html.

The Odessa Journal. 2023. "Ukrainian developers have created the Mantis Analytics platform based on artificial intelligence." Odessa-Journal.com, September 14. https://odessa-journal.com/ukrainian-developers-have-created-the-mantis-analytics-platform-based-on-artificial-intelligence#google_vignette.

The Recursive. 2025. "Ukrainian Startup LetsData Raises €1,5M to Fight Disinformation with AI." News, January 15. https://therecursive.com/ukrainian-startup-letsdata-raises-e1-5m-to-fight-disinformation-with-ai/.

Twomey, John G., Didier Ching, Matthew P. Aylett, Michael Quayle, Conor Linehan and Gillian Murphy. 2023. “Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine.” *PLOS One* 18 (10): e0291668. https://doi.org/10.1371/journal.pone.0291668.

Ukrinform. 2025. “В Україні почали розробку власної великої мовної моделі ШІ.” Ukrinform.ua, June 17. www.ukrinform.ua/rubric-economy/4005333-v-ukraini-pocali-rozrobku-vlasnoi-velikoi-movnoi-modeli-si.html.

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