ECONOMISTS
FOR UKRAINE

POLICY BRIEF #1

Democracy Under Pressure: Strengthening EU Defences Against Russian Disinformation

Egor Bronnikov, Tatyana Deryugina, Jon Roozenbeek, and Sander van der Linden[1]

Executive Summary

Key messages

1. Russian state-sponsored disinformation campaigns targeting Europe aim to erode trust, increase polarisation, and weaken collective decision-making in democratic societies.
2. These campaigns are coordinated, adaptive, and sustained over time, making fragmented, reactive responses ill-suited to counter them.
3. State-sponsored disinformation is part of a broader strategy to weaken democracies, alongside attacks on information and energy infrastructure. Russia treats these as a unified doctrine integrating information and kinetic warfare.
4. Democratic openness creates a structural asymmetry: while authoritarian regimes can weaponize information with few constraints, democracies must safeguard rights and free expression, making them vulnerable to large-scale exploitation and confusion unless they invest in long-term resilience.

Core recommendations

1. Treat Russia's state-sponsored disinformation as a persistent security and democratic resilience challenge and recognize that countering it requires a preemptive and proactive approach.
2. Strengthen coordination across EU member states and institutions to develop state-of-the-art responses to disinformation, systematically sharing lessons learned, benchmarking performance, and continuously refining best practices through joint evaluation and iterative improvement.
3. Develop a comprehensive, evidence-based education strategy on disinformation that draws on best-in-class European models (e.g., Sweden and Finland), rigorously evaluates outcomes, and scales the most effective approach.

[1] Egor Bronnikov is a doctoral researcher at Maastricht University, a Malyi Visiting Fellow at the University of Chicago, and an adjunct professor at Brīvā Universitāte. Tatyana Deryugina is an Associate Professor of Finance at the University of Illinois. Jon Roozenbeek is an Associate Professor at the University of Cambridge and the Vrije Universiteit Amsterdam. Sander van der Linden is a Professor of Psychology at the University of Cambridge.

An Overview of Russian Disinformation Operations

Background

While disinformation has existed for centuries, its capacity to spread rapidly around the world has grown with the rise of digital media, reflecting changes in contemporary information environments. High volumes of content, heightened emotional salience, rapid diffusion, and fragmented political and social communities can foster individuals' reliance on cognitive heuristics such as repetition, social endorsement, and identity cues (Ecker et al. 2022). At the same time, institutions struggle to respond to disinformation with aligned and authoritative signals (Bleyer-Simon et al. 2025), particularly when many platforms' designs privilege engagement over accuracy (Gauthier et al. 2026), allowing misleading content to spread more quickly than corrective information (Vosoughi et al. 2018).

Russian disinformation operations have deep roots in Soviet-era "active measures" and reflexive control doctrine.

From an institutional perspective, democracies are particularly vulnerable to disinformation campaigns because commitments to free expression constrain blunt suppression, and baseline trust in institutions has already declined (OECD 2025). Russia does not necessarily create these vulnerabilities, but it certainly exploits and amplifies those that already exist.

Russian disinformation operations have deep roots in Soviet-era "active measures" and reflexive control doctrine (Rid 2020, Global Engagement Center 2021). Both were designed to covertly shape perceptions, exploit uncertainty, and steer opponents' choices in ways favourable to Russian strategic interests. A well-known example is Operation Denver, the Soviet AIDS disinformation campaign in which the KGB successfully spread the false claim that HIV/AIDS originated from U.S. bioweapons research (Selvage 2019). Since at least the mid-2000s—and with increased intensity after 2014—these Soviet-era practices have been modernised through digital platforms, data-driven targeting, and cross-platform amplification.

This brief focuses on Russian disinformation targeting foreign audiences, particularly in Europe. Russia also conducts extensive domestic information control and manipulation, but that lies beyond the scope of this analysis.

Strategic Objectives

Russian foreign information manipulation and interference (FIMI) is not primarily aimed at convincing audiences of a single (false) narrative (Roozenbeek, 2024). Instead, its primary objectives include:

1. **Undermining trust** in democratic institutions, including media, elections, public authorities, and knowledge;
2. **Intensifying polarization** and social conflict within target societies;
3. **Generating confusion**, where competing claims erode the distinction between fact, opinion, and fabrication;
4. **Weakening collective action capacity** in democratic states by fostering cynicism, disengagement, and fatigue;
5. **Advancing geopolitical objectives indirectly** by constraining opponents' ability to respond coherently to Russia's hostile actions.

Foreign information manipulation and interference is an integral component of Russian hybrid warfare and military strategy, used to prepare the informational environment for coercive or kinetic action.

FIMI is an integral component of Russian hybrid warfare and military strategy, used to prepare the informational environment for coercive or kinetic action. This approach is often referred to in Western analysis as the "Gerasimov doctrine", after Valery Gerasimov, Chief of the General Staff of the Armed Forces of the Russian Federation. It conceptualizes information warfare as a critical element of kinetic warfare (Gerasimov 2016). Within this framework, disinformation operates alongside attacks on information infrastructure (e.g., internet cables) and the use of informational architectures to disrupt operational capacities (e.g., cyberattacks on energy installations such as NotPetya). Russia's war against Ukraine represents the clearest contemporary example of this integrated approach. Recorded incidents also show sustained targeting of EU Member States, NATO allies, and G7 partners, particularly around elections, sanctions and energy policy, and security commitments (European External Action Service, 2026).

Organisational and Infrastructural Architecture

State-sponsored disinformation campaigns combine scale, coordination, deniability, and strategic alignment with geopolitical objectives. Russia's information manipulation system is the product of sustained investment rather than opportunistic activity. It is best understood as distributed, layered, and plausibly deniable, rather than operating as a single, centrally run operation (U.S. Department of State 2020; EUvsDisinfo 2025; Odarchenko 2025; Voo and Singh 2025). This multi-layered "ecosystem" provides the Russian disinformation system with both resilience and deniability: the disruption of individual nodes does not meaningfully degrade overall operational capacity.

Strategic direction is provided at the political level, notably through the Presidential Administration, while different state and quasi-state

actors perform distinct operational roles. For example, security services such as the FSB and GRU are associated with covert and plausibly deniable activities, while institutions like the Ministry of Foreign Affairs are used for overt narrative positioning and diplomatic amplification.

State-owned and state-controlled media are a core component of this ecosystem. Outlets such as RT and Sputnik produce professionally packaged content that disproportionately targets foreign audiences. To maintain surface credibility, this content often blends factual reporting with selective framing, omission, and false equivalence, allowing narratives to circulate beyond explicitly pro-Kremlin channels (Tolz and Teper 2018).

To maintain surface credibility, state-controlled media content often blends factual reporting with selective framing, omission, and false equivalence.

Beyond formal state actors, the system incorporates a wide range of intermediaries, including contractors, shell companies, NGOs, vendors of manipulation services such as bot accounts, networks of inauthentic websites, and nominally independent influencers and commentators who are either ideologically aligned or financially incentivised. European External Action Service (EEAS) investigations into Russian disinformation operations document a vast online infrastructure involving coordinated activity across thousands of channels and multiple languages (EEAS 2024). This infrastructure includes inauthentic domains, platform accounts, cloned or inauthentic websites (Dek et al. 2025), coordinated inauthentic behaviour networks, paid amplification accounts, and proxy channels used to redistribute state-linked content across multiple platforms.

An underlying commercial infrastructure sustains this and other large-scale inauthentic activity. Recent research mapping the “online manipulation economy” demonstrates that mass account creation (including by disinformation actors) relies on a thriving transnational gray market in on-demand SMS verifications (an essential component of account registration), which enables actors to circumvent platform identity safeguards at scale (Dek et al. 2025). Service providers bulk-purchase physical or virtual SIM cards and resell verification codes for hundreds of platforms, effectively supplying the raw inputs for industrialized account registration across jurisdictions. In addition, vendors on this marketplace sell downstream services such as fake likes, comments, and wholesale bot armies. This market-based infrastructure constitutes a structural enabler of disinformation campaigns: it reduces entry barriers, supports scalability, and facilitates rapid network reconstitution after takedowns.

Methods and Operational Patterns

Operationally, Russian campaigns display the features described in RAND's "firehose of falsehood" model, characterised by large-scale dissemination, rapid and repetitive circulation, use of multiple channels, and a strategic indifference to credibility or internal consistency (Paul and Matthews 2016). Rather than promoting a single version of events, campaigns frequently circulate multiple, mutually contradictory narratives simultaneously. The aim is not to produce conclusive belief, but to generate doubt, confusion, and informational exhaustion. A well-documented example is the response to the downing of Malaysia Airlines Flight MH17 in 2014, where Russian-linked outlets promoted competing explanations—including Ukrainian responsibility, Western fabrication, and staged events—within the same news cycle (Mölder and Sazonov 2019). Similar patterns recur across other information operations such as debates about racial issues (Freelon et al. 2022) or vaccination (Broniatowski et al. 2018).

The aim of Russian disinformation campaigns is not to produce conclusive belief, but to generate doubt, confusion, and informational exhaustion.

A complementary tactic is "information laundering", which helps misleading narratives migrate from marginal or fabricated sources into broader public discourse (Toucas 2017). Rather than relying solely on overt state outlets, campaigns often introduce a claim through cloned websites, anonymous blogs, or loosely affiliated platforms, after which it is amplified by coordinated social media accounts and cross-referenced across multiple domains. Through repetition, citation, and platform hopping, the original source becomes obscured, and the narrative acquires the appearance of independent corroboration. Over time, such content may be referenced by commentators or secondary outlets that treat it as externally validated information. This layered circulation complicates debunking efforts and increases the probability that misleading claims penetrate mainstream information ecosystems without appearing directly state-sponsored.

Russian disinformation initiatives such as *Doppelgänger* and *False Facade* highlight the operational sophistication and procedural discipline underpinning such campaigns. They involve systematic domain cloning to mimic trusted brands, synchronized posting schedules across platforms, coordinated inauthentic engagement to trigger algorithmic amplification, and the strategic use of paid advertising to seed narratives into targeted audiences. These operations also rely on redundancy and rapid reconstitution: pre-positioned backup domains and accounts allow narratives to persist even after takedowns.

Content design systematically exploits emotional triggers such as anger, fear, grievance, and identity threat, which are known to increase sharing and reduce analytical scrutiny (McLoughlin et al. 2024). Narratives often begin with real or partially real grievances, such as inequality or corruption, which are then selectively amplified, reframed, and attributed in ways that depict democratic systems as irredeemably hypocritical or dysfunctional. Micro-segmentation allows different—and sometimes opposing—messages to be tailored to distinct audiences, increasing conflict and fragmentation.

The pervasiveness and effectiveness of Russian disinformation campaigns may not be as large as widely assumed (e.g., Alizadeh et al. 2020, Bail et al. 2020, Guess et al. 2020, Eady et al. 2023). Additionally, any effects such campaigns do have (e.g., Ruck et al. 2019) derive less from informational sophistication than from their alignment with well-documented cognitive and institutional constraints. These include truth-default bias (people assume sincerity), confirmation bias (people believe what fits identity), overconfidence in deception detection (people overestimate their ability to spot falsehoods), and attention scarcity in high-information environments (limited cognitive bandwidth reduces careful scrutiny and increases reliance on heuristics) (e.g., Allcott and Gentzkow 2017, Pantazi et al. 2018, Levine 2019, Pennycook and Rand 2019, Serra-Garcia and Gneezy 2021). Success is measured not by narrative dominance, but by disengagement, erosion of trust, and the normalization of moral and epistemic relativism.

Responding effectively to sustained Russian state-sponsored disinformation requires treating it as a persistent security and democratic resilience challenge rather than episodic misinformation.

A Resilience Framework for Democratic Defence

Responding effectively to sustained Russian state-sponsored disinformation requires treating it as a persistent security and democratic resilience challenge rather than episodic misinformation. Because these campaigns are continuous, adaptive, and strategically aligned with geopolitical objectives, countermeasures must be institutionalised and sustained over time. The objective is not to "win" individual narrative disputes, but to build and maintain a system capable of continuously managing and absorbing manipulation attempts.

An effective resilience strategy also requires calibrated threat assessment. Russian state-sponsored disinformation should be treated seriously not because it reflects uniquely sophisticated or unbeatable capabilities but because of its scale, persistence, and coordination. Much of its impact derives from volume, repetition, and exploitation of existing vulnerabilities rather than technical brilliance or persuasive ingenuity. Overstating its sophistication or impact risks

reinforcing the very narrative of strategic omnipotence that Russian information operations seek to project. Inflating the threat can induce fatalism, policy overreach, or misplaced deference to the adversary's supposed capabilities. A sober assessment recognises that these campaigns are resource-intensive and sustained, but often tactically crude and reliant on commercially available tools and predictable manipulation techniques. The appropriate response is therefore neither complacency nor alarmism, but sustained, proportionate, and evidence-based resilience.

The appropriate response to Russian disinformation operations is neither complacency nor alarmism, but sustained, proportionate, and evidence-based resilience.

Such a system should rest on three interlocking pillars.

1. **Permanent institutional capacity**. To combat Russian disinformation effectively, the EU and its Member States need standing analytical, coordination, and response capabilities that operate across electoral cycles and crisis periods. This means embedding monitoring, cross-platform analysis, and rapid information-sharing into routine governance structures rather than activating them only during or after high-profile events. Treating disinformation as a structural threat implies sustained funding, continuity of expertise, and clear institutional mandates.

2. **Structured coordination and continuous improvement**. Given the cross-border and cross-platform nature of Russian operations, resilience depends on systematic coordination across EU institutions and Member States. This includes implementing shared standards for identifying state-linked manipulation, joint evaluation of interventions, benchmarking of national approaches, and regular exchange of lessons learned. Responses should be iteratively refined based on evidence, with mechanisms for comparing performance and scaling effective practices across jurisdictions.

3. **Long-term education and societal resilience**. Member States, supported by EU coordination, should rigorously assess the effectiveness of existing media literacy and disinformation-awareness programmes, using comparable metrics and evidence-based standards. Interventions that demonstrably improve resistance to manipulation should be identified and scaled, while ineffective approaches should be revised or discontinued. Building on this evaluation framework, the EU can draw on best-practice models such as those developed in Sweden and Finland to design a comprehensive, evidence-based education strategy. Integrating structured media literacy and awareness of state information warfare into formal education, public service

training, and adult learning will ensure that resilience-building is cumulative, measurable, and evidence-based rather than dispersed across untested initiatives.

Together, these elements define a resilience architecture that matches the persistence, coordination, and adaptability of Russian disinformation campaigns. As the next section discusses, the question for European policymakers is not whether relevant tools exist, but whether they are integrated, permanent, and proportionate to the scale of the challenge.

A potential objection to strengthening counter-disinformation measures is that Russia will simply adapt—shifting narratives, platforms, and tactics—forcing democracies into a perpetual game of catch-up. This attitude overlooks three important points. First, adaptation is costly: rebuilding networks, responding to educational initiatives, and evading platform enforcement or regulatory scrutiny requires time and resources and involves operational risk. Countermeasures can meaningfully raise those costs and reduce reach, even if they do not eliminate the threat entirely. Second, the need for continual adjustment is not a reason for passivity; policymakers already accept this dynamic in domains such as cybersecurity, counterterrorism, and financial crime, where defences are continuously updated in response to evolving tactics. Third, the alternative to sustained engagement is far worse: allowing Russia to degrade Europe's information environment, erode public trust, polarize democratic societies, and interfere with elections at scale. There is little evidence that disinformation campaigns dissipate on their own; absent persistent and coordinated countermeasures, they tend to adapt, entrench, and expand.

The question for European policymakers is not whether relevant tools to combat Russian disinformation exist, but whether they are integrated, permanent, and proportionate to the scale of the challenge.

Existing European Systems of Disinformation Protection

European responses to disinformation address important components of resilience, but they remain functionally fragmented when assessed against the framework outlined above. Existing initiatives can be grouped into four core functions: monitoring and attribution; research and evidence generation; crisis communication; and long-term education and societal resilience. While each function is partially developed, they do not yet operate as an integrated, standing capability proportionate to sustained state-led campaigns. A comparison of Russian investment in disinformation operations and European spending on countermeasures also highlights a significant imbalance in scale that requires correction.

1. Monitoring and Attribution

The most established EU-level effort is EUvsDisinfo, operated by the East StratCom Task Force within the European External Action Service. Since 2015, it has systematically documented and analysed foreign disinformation campaigns—particularly pro-Kremlin narratives—and increased transparency through public databases and weekly reviews. Its strength lies in visibility and in attributing disinformation to specific state or state-linked actors. However, its mandate remains primarily analytical and communicative rather than operational or preventive.

At the national level, France's Service for Vigilance and Protection against Foreign Digital Interference (VIGINUM), established in 2021, provides a rule-based mechanism for detecting and characterising foreign digital interference. It demonstrates that systematic identification of coordinated inauthentic behaviour can operate within democratic legal constraints. However, its remit focuses on detection rather than broader societal resilience. Together, monitoring and attribution improve transparency and situational awareness but do not themselves constitute a standing cross-border response system.

Monitoring and attribution improve transparency and situational awareness but do not themselves constitute a standing cross-border response system.

2. Research and Evidence Generation

The European Digital Media Observatory (EDMO) connects fact-checkers, researchers, and media literacy practitioners across Member States. It has generated practical outputs, including prebunking-oriented materials related to emerging risks such as AI-generated disinformation ahead of elections. EDMO strengthens the analytical and research ecosystem but operates as a distributed observatory rather than a permanent operational capability.

The European Commission's Joint Research Centre (JRC) further contributes by analysing the effectiveness of prebunking and debunking strategies, helping translate behavioural science into policy-relevant insights (e.g., Nyhan and Reifler, 2010; Roozenbeek and Van der Linden, 2019, 2024; Van der Linden, 2022; Roozenbeek et al., 2022). However, this work remains advisory rather than institutionalised as a continuous resilience function.

3. Crisis Communication and Trusted Information Hubs

A partial analogue to trusted crisis information infrastructure emerged during the COVID-19 pandemic with Re-open EU, a centralised platform providing regularly updated cross-border information. Re-open EU demonstrated the value of a single authoritative reference point during periods of high uncertainty and

rapid information flows. However, it was crisis-specific and time-limited, rather than a permanent, all-hazards information capability.

Evidence-based communication methods such as prebunking have also been deployed operationally during other crises. Prior to Russia's 2022 invasion of Ukraine, the United States and United Kingdom publicly released intelligence to expose anticipated false-flag operations and fabricated pretexts, thereby pre-empting key narratives and helping sustain allied cohesion (The Economist 2022). Although this did not prevent the invasion, it complicated Russia's information strategy and provided time for diplomatic and military preparation. Similar approaches were used in other contexts, including publicizing a covert disinformation campaign in Central and South America (Myers 2023) and prebunking deepfake videos falsely depicting President Zelenskyy announcing surrender (The Guardian 2022).

However, these efforts were ad-hoc rather than part of a broader anti-disinformation system. No equivalent standing EU-level mechanism currently exists to provide consolidated, authoritative communication during periods of heightened foreign information manipulation, such as elections, sanctions escalations, or geopolitical crises.

No standing EU-level mechanism currently exists to provide consolidated, authoritative communication during periods of heightened foreign information manipulation.

4. Long-Term Education and Societal Resilience

In the education domain, the European Commission has issued guidance and toolkits for teachers and supported coordination through the European Digital Education Hub. These initiatives contribute to long-term resilience but rely on soft coordination and project-based funding instruments.

Several Member States provide instructive national models. Sweden's Psychological Defence Agency integrates analysis, public guidance, and institutional coordination to counter foreign malign information influence, offering a close national analogue to a resilience-centred approach. Finland's long-standing integration of media literacy into its education system demonstrates how durable resilience can be built without politicising content or restricting expression. During the COVID-19 pandemic, the United Kingdom deployed dedicated counter-disinformation units and developed the RESIST toolkit, illustrating how structured response frameworks can operate during acute crises.

These examples show that resilience-oriented approaches are institutionally feasible within democratic systems. However, they remain nationally bounded and unevenly distributed across the EU.

Comparative expenditures

Available budgetary data indicate a clear imbalance between the resources Russia devotes to information influence activities and those European institutions devote to countering them. Even before the full-scale invasion, Russian federal budgets allocated over €1 billion annually to state-controlled media alone, including major international broadcasters such as RT and the Rossiya Segodnya/Sputnik network. Individual organizations receive very large recurring subsidies. For example, RT has received over €350 million per year in recent budgets. The 2025 and 2026 budgets each included about €1.5 billion for state-controlled news agencies and television, an increase of almost 30 percent compared to 2021 (Kravchuk 2024; Langford, 2025). Project Lakhta, a Russian influence operation that included the Internet Research Agency (IRA), had a monthly budget of $1.25 million. The Main Intelligence Directorate of the General Staff (GRU), the Foreign Intelligence Service (SVR), and the Federal Security Service (FSB) also conduct disinformation operations, although it is not feasible to separately quantify their costs. Russian state-affiliated think tanks and policy organizations—including the Valdai Discussion Club, the Russian International Affairs Council, the Russian Institute for Strategic Studies, the Institute of World Economy and International Relations, and related entities—also contribute to these influence and messaging efforts, though their costs similarly cannot be quantified explicitly. Nonetheless, the cumulative evidence points to a well-resourced, institutionalized ecosystem in which substantial and sustained state funding underwrites Russia's disinformation capabilities at scale.

By contrast, identifiable European spending on counter-disinformation initiatives is smaller and more fragmented across programs. EU-level efforts—including the East StratCom Task Force (EUvsDisinfo), the European Digital Media Observatory (EDMO), and research and media-literacy programs funded through Horizon Europe and related instruments—generally involve budgets in the €2–11 million range per initiative. Even when aggregated across these programs, total identifiable EU-level spending amounts to tens of millions to low hundreds of millions of euros, substantially below the annual funding devoted to Russian state media. This disparity highlights the structural asymmetry confronting democratic responses: Russia concentrates large, sustained resources in centralized state media institutions, while European responses currently rely on a distributed set of smaller monitoring, research, and resilience programs.

Russia concentrates large, sustained resources in centralized state media institutions, while European responses currently rely on a distributed set of smaller monitoring, research, and resilience programs.

Conclusion

Russian state-sponsored disinformation is not a transient communications problem but a persistent feature of contemporary geopolitical competition. Its impact derives less from technical sophistication than from scale, coordination, and the systematic exploitation of structural vulnerabilities within democratic information environments. Addressing it therefore requires neither emergency powers nor episodic counter-messaging, but durable institutional design.

The European Union and its Member States already possess many of the necessary components: monitoring capacity, research expertise, educational initiatives, and crisis-time precedents. What remains lacking is integration, permanence, and systematic coordination proportionate to the scale and persistence of the threat. Treating Russian disinformation as a standing resilience challenge, strengthening cross-border coordination and iterative improvement, and grounding education policy in rigorous evaluation are practical and achievable steps. The objective is not to eliminate manipulation altogether, but to raise its costs, limit its reach, and ensure that democratic institutions remain capable of coherent and collective action in the face of sustained information pressure.

References

Alizadeh, M., Shapiro, J. N., Buntain, C., & Tucker, J. A. (2020). Content-based features predict social media influence operations. *Science Advances, 6*(30), eabb5824.

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives, 31*(2), 211–236.

Bail, C. A., Guay, B., Maloney, E., Combs, A., Hillygus, D. S., Merhout, F., ... Volfovsky, A. (2020). Assessing the Russian Internet Research Agency's impact on the political attitudes and behaviors of American Twitter users in late 2017. *Proceedings of the National Academy of Sciences, 117*(1), 243–250.

Bavel, J. J. van, Baicker, K., Boggio, P. S., Capraro, V., Cichocka, A., Cikara, M., et al. (2020). Using social and behavioural science to support COVID-19 pandemic response. *Nature Human Behaviour, 4*(5), 460–471.

Berinsky, A. J. (2017). Rumors and health care reform: Experiments in political misinformation. *British Journal of Political Science, 47*(2), 241–262.

Berinsky, A. J. (2023). *Political rumors: Why we accept misinformation and how to fight it*. Princeton University Press.

Bleyer-Simon, K., Aslama Horowitz, M., Botan, M., Brautovic, M., Brogi, E., Bucholtz, I., Culloty, E., Gavurova, B., Grabovac, A., Ioakem, S., Kermer, J. E., Kiely, K., Leonidou, P., Mallia, M., Moreno, J., Nenadić, I., Paisana, M., Palmer, M., Reviglio, U., Magallón Rosa, R., Salamanos, N., Salaverría Aliaga, R., Sessa, M. G., Sitistas, T., & Soukupová, J. (2025). *How is disinformation addressed in the member states of the European Union? – 27 country cases*. European Digital Media Observatory (EDMO). Available at: https://edmo.eu/wp-content/uploads/2025/06/EDMO-Report-How-is-disinformation-addressed-in-the-member-states-of-the-European-Union-%E2%80%93-27-country-cases-.pdf (Accessed: 13 March 2026).

Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., Quinn, S. C., & Dredze, M. (2018). Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate. *American Journal of Public Health, 108*(10), 1378–1384.

Dek, A., Kyrychenko, Y., van der Linden, S., & Roozenbeek, J. (2025). Mapping the online manipulation economy. *Science, 390*(6778).

Eady, G., Paskhalis, T., Zilinsky, J., Bonneau, R., Nagler, J., & Tucker, J. A. (2023). Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior. *Nature Communications, 14*(1), 62.

Ecker, U. K. H., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N., et al. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology, 1*.

Economist, The. (2022). Deploying reality against Putin. Available at: https://www.economist.com/united-states/2022/02/26/deploying-reality-against-putin

EUvsDisinfo. (2025). Exposing and analysing Russia's FIMI operations. European External Action Service. https://euvsdisinfo.eu/exposing-and-analysing-russias-fimi-operations/

European External Action Service (EEAS). (2024). *2nd EEAS report on foreign information manipulation and interference (FIMI) threats: A framework for networked defence*. Brussels: European External Action Service. Available at:

https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

European External Action Service. (2026). Information integrity and countering foreign information manipulation and interference (FIMI). Available at: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en (Accessed: 13 March 2026).

Freelon, D., Bossetta, M., Wells, C., Lukito, J., Xia, Y., & Adams, K. (2022). Black trolls matter: Racial and ideological asymmetries in social media disinformation. *Social Science Computer Review, 40*(3), 560–578.

Gauthier, G., Hodler, R., Widmer, P., & Zhuravskaya, E. (2026). The political effects of X's feed algorithm. *Nature*.

Gerasimov, V. (2016). The value of science is in the foresight: New challenges demand rethinking the forms and methods of carrying out combat operations. *Military Review*, January–February, 23–29.

Global Engagement Center. (2021). The goals and main tactics of Russia's disinformation. *GEC Counter-Disinformation Dispatches #11*. U.S. Department of State. Available at: https://e.america.gov/t/ViewEmail/i/CD46E76EEAD07F9E2540EF23F30FEDED (Accessed: March 21, 2026).

Guardian, The. (2022). Deepfakes v pre-bunking: Is Russia losing the infowar? Available at: https://www.theguardian.com/world/2022/mar/19/russia-ukraine-infowar-deepfakes

Guess, A. M., Nyhan, B., & Reifler, J. (2020). Exposure to untrustworthy websites in the 2016 US election. *Nature Human Behaviour, 4*(5), 472–480.

Kravchuk, V. (2024). Russia to spend $118 million per month on state propaganda in 2025. *Euromaidan Press*.

Langford, A. (2025). Kremlin pours record sums into state propaganda. *Kyiv Post*.

Levine, T. R. (2019). *Duped: Truth-default theory and the social science of lying and deception*. University of Alabama Press.

Linegar, M., Sinclair, B., van der Linden, S., & Alvarez, R. M. (2024). Prebunking elections rumors: Artificial intelligence assisted interventions increase confidence in American elections. *arXiv preprint arXiv:2410.19202*.

McLoughlin, K. L., Brady, W. J., Goolsbee, A., Kaiser, B., Klonick, K., & Crockett, M. J. (2024). Misinformation exploits outrage to spread online. *Science, 386*(6725), 991–996.

Microsoft Threat Analysis Center (MTAC). (2024). *Lead-up to Election Day 2024: Russia, Iran, and China engaging in influence activity in the first U.S. election cycle of its kind*. Microsoft Threat Intelligence Report.

Mölder, H., & Sazonov, V. (2019). The impact of Russian anti-Western conspiracy theories on the status-related conflict in Ukraine: The case of Flight MH17. *Baltic Journal of European Studies, 9*(3), 96–115.

Myers, S. (2023). U.S. tries new tack on Russian disinformation: Pre-empting it. *The New York Times*.

Nyhan, B., & Reifler, J. (2010). When corrections fail: The persistence of political misperceptions. *Political Behavior, 32*(2), 303–330.

Odarchenko, K. (2025). The fight against disinformation: A persistent challenge for democracy. *Foreign Policy Research Institute*. https://www.fpri.org/article/2025/01/the-fight-against-disinformation-a-persistent-challenge-for-democracy/

Organisation for Economic Co-operation and Development (OECD). (2025). Levels of trust in public institutions. In *Government at a glance 2025*. Available at: https://www.oecd.org/en/publications/2025/06/government-at-a-glance-2025_70e14c6c/full-report/levels-of-trust-in-public-institutions_62a3b94e.html (Accessed: 13 March 2026).

Pantazi, M., Kissine, M., & Klein, O. (2018). The power of the truth bias: False information affects memory and judgment even in the absence of distraction. *Social Cognition, 36*(2), 167–198.

Paul, C., & Matthews, M. (2016). The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it. RAND Corporation. Available at: https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf (Accessed: March 21, 2026).

Pennycook, G., & Rand, D. G. (2019). Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. *Cognition, 188*, 39–50.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Profile Books.

Roozenbeek, J., & van der Linden, S. (2019). Fake news game confers psychological resistance against online misinformation. *Palgrave Communications, 5*(1).

Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S., & Lewandowsky, S. (2022). Psychological inoculation improves resilience against misinformation on social media. *Science Advances, 8*(34).

Roozenbeek, J., & van der Linden, S. (2024). *The psychology of misinformation*. Cambridge University Press.

Roozenbeek, J. (2024). *Propaganda and ideology in the Russian–Ukrainian war*. Cambridge University Press.

Ruck, D. J., Rice, N. M., Borycz, J., & Bentley, R. A. (2019). Internet Research Agency Twitter activity predicted 2016 US election polls. *First Monday, 24*(7).

Selvage, D. (2019). Operation 'Denver': The East German Ministry of State Security and the KGB's AIDS disinformation campaign, 1985–1986 (Part 1). *Journal of Cold War Studies, 21*(4), 71–123.

Serra-Garcia, M., & Gneezy, U. (2021). Mistakes, overconfidence, and the effect of sharing on detecting lies. *American Economic Review, 111*(10), 3160–3183.

Tolz, V., & Teper, Y. (2018). Broadcasting agitainment: A new media strategy of Putin's third presidency. *Post-Soviet Affairs, 34*(4), 213–227.

Toucas, B. (2017). Exploring the information-laundering ecosystem: The Russian case. Center for Strategic and International Studies. Available at: https://www.csis.org/analysis/exploring-information-laundering-ecosystem-russian-case (Accessed: March 21, 2026).

U.S. Department of State, Global Engagement Center. (2020). *Pillars of Russia's disinformation and propaganda ecosystem*. https://2021-2025.state.gov/russias-pillars-of-disinformation-and-propaganda-report/?safe=1

van der Bles, A. M., van der Linden, S., Freeman, A. L., Mitchell, J., Galvao, A. B., Zaval, L., & Spiegelhalter, D. J. (2019). Communicating uncertainty about facts, numbers and science. *Royal Society Open Science, 6*(5), 181870.

van der Bles, A. M., van der Linden, S., Freeman, A. L., & Spiegelhalter, D. J. (2020). The effects of communicating uncertainty on public trust in facts and numbers. *Proceedings of the National Academy of Sciences, 117*(14), 7672–7683.

van der Linden, S. (2022). Misinformation: Susceptibility, spread, and interventions to immunize the public. *Nature Medicine, 28*(3), 460–467.

Voo, J., & Singh, V. V. (2025). Russia's information confrontation ecosystem. International Institute for Strategic Studies. https://www.iiss.org/charting-cyberspace/2025/06/russias-information-confrontation-ecosystem/

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151.

About Economists for Ukraine

Economists for Ukraine is a collective of economists and members of the global academic community dedicated to supporting Ukraine in response to Russia's invasion. The organization focuses on advancing policies that strengthen Ukraine's resilience, contribute to the cessation of hostilities, and support long-term reconstruction and economic stability. It operates as the think tank arm of the AI for Good Foundation, a global non-profit organization focused on leveraging technology to address major societal challenges.

The group brings together expertise across macroeconomics, finance, behavioral economics, environmental economics, governance, and game theory to produce policy-relevant analysis. Its work includes research publications, policy briefs, and collaboration with initiatives such as the International Working Group on Russian Sanctions, with the aim of informing effective economic and financial measures targeting the Russian economy.

In addition to analytical work, Economists for Ukraine contributes to practical recovery efforts. In coordination with the AI for Good Foundation, Ukrainian government institutions, and local partners, the organization supports initiatives addressing urgent humanitarian needs and longer-term reconstruction priorities.