BFMI
BALKAN FREE MEDIA INITIATIVE

SENSIKA

Tackling 'TikTokcracy' in the Balkans:

A blueprint for fighting algorithmic-manipulation in Europe

Table of Contents

Foreword

Eric Jozsef,
Journalist with Libération, author and co-founder of EuropaNow!

When Romania's presidential election was annulled, Europe crossed a threshold, as algorithms were weaponised to reshape the course of history. For the first time, a democratic process fell to systemic digital manipulation rather than ballot fraud. This is Europe's wake-up call. The information space has become a second front in the defence of our democracies, and we are not prepared.

The security implications extend far beyond electoral outcomes. Non-transparent financing of disinformation networks creates pathways for money laundering and corruption. The erosion of independent and credible media robs citizens of accountability mechanisms and erodes the trust necessary for democratic governance. In polarised societies without institutional mediation, these influence operations weaken democracy and create conditions for instability and conflict.

The Balkans, with a legacy of media capture and post-conflict vulnerabilities, has become a testing ground for algorithmic manipulation. What succeeds there will be deployed elsewhere. Foreign actors exploit regulatory gaps and democratic disillusionment in this region as a gateway to assault Europe's broader information system. What happens in the Balkans today may well anticipate what Europe will face tomorrow.

The tactics that proved effective in Romania failed in Moldova last month, as society was clear-eyed to the risks of digital manipulation. Thanks to massive civic engagement and proactive cooperation among institutions, platforms and media, Moldova reminds us that manipulation is not inevitable, and resilience can be built.

This report provides a defensive map that connects traditional and digital media, aligns old and new regulatory tools, and deploys all elements of democratic defence in concert. Like any effective combined operation, success depends on clear direction, integrated execution, and ensuring that all defensive units play their part. Old and new media must be deployed coherently, with platforms and regulators, civil society and independent media all working from the same strategic plan.

Europe cannot rely on twentieth-century mechanisms to address twenty-first-century threats. The European Commission's Democracy Shield initiative provides a promising foundation. What is now required is determined implementation, guided by evidence, rooted in rights and supported by sustained investment in media independence.

Europe's leaders, both at the national and EU levels, may see in these recommendations a chance to renew our collective commitment to democratic resilience. The work ahead is to restore confidence in the institutions and in the independent media that sustain open societies, so that Europe remains steadfast and self-assured in the face of manipulation. To strengthen democracy is not an act of confrontation but an affirmation of Europe's enduring values and its devotion to transparency, accountability and trust.

Executive Summary

In December 2024, Romania annulled its presidential vote after discovering that tens of thousands of fake TikTok accounts had propelled a pro-Russian candidate from obscurity to victory. This moment exposed a rapidly-approaching reality, in which democracy risks becoming "TikTokcracy," ruled by clicks and sensationalism rather than truth and deliberation. Europe now faces a stark choice: ask democracies to go against established processes and procedures in order to save themselves from foreign interference or completely reimagine democratic defence to meet the current moment.

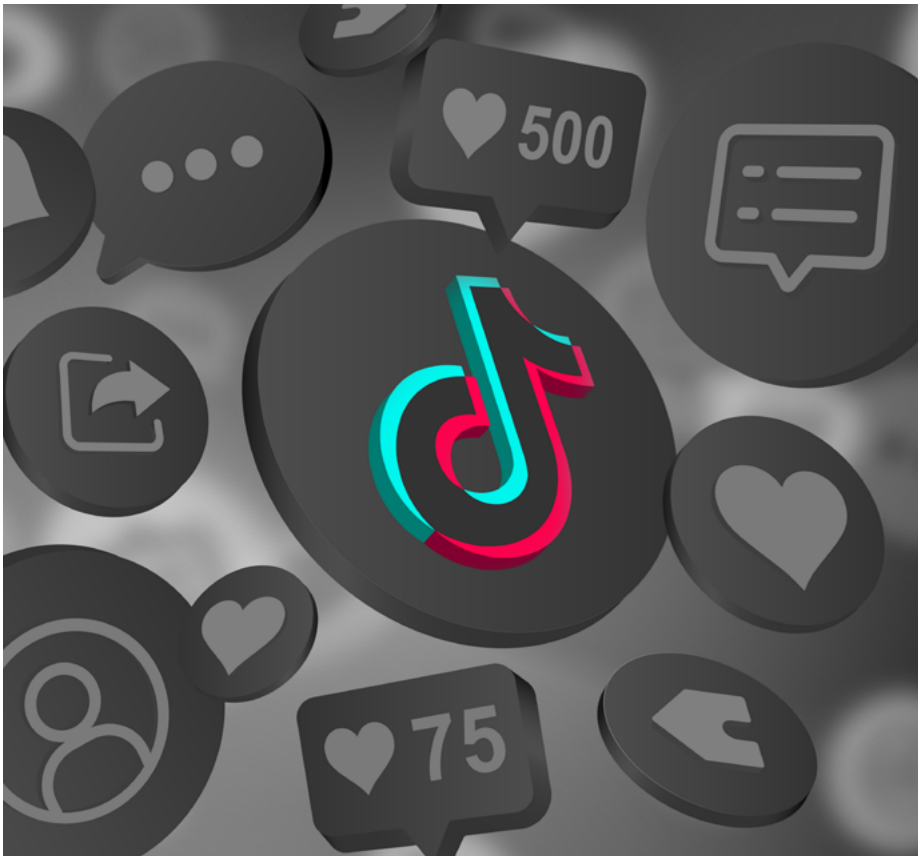
This report provides a blueprint for Europe to move away from reactive crisis management to anticipatory democratic defence. By linking regulation, technology and credible media into a single protective ecosystem, this report shows how Europe can safeguard its open societies against the weaponisation of information. As the tempo of online manipulation rapidly accelerates, the need for such a transformation is increasingly urgent. While the authors of this report believe that the European Commission's Democracy Shield (EUDS) initiative is a useful starting point for this transformation, our findings underscore that the EUDS requires rapid and aggressive amplification and delivery to address realities on the ground.

The threat of TikTokcracy is fundamentally borderless, necessitating a response that is cross-border and multi-stakeholder. The case studies detailed here indicate that the events of the 2024-2025 Romanian presidential elections were not isolated developments. Rather, Romania's experience exposed structural vulnerabilities across Europe's information space, ones shared by fellow member states like Bulgaria and prospective members like Kosovo.

In each of these cases, inauthentic activity, coordinated behaviour and unmarked content were used by political actors, their supporters and paid influencers to artificially boost engagement for certain parties, candidates and narratives around peak election periods in 2024 and 2025. Given that Romania, Bulgaria and Kosovo have some of the highest rates of TikTok penetration in all of Europe, these cases pose a clear warning of where other countries may be headed without immediate attention from Brussels and its partners across sectors. From these case studies, the following key recommendations emerged, and are applicable to countries across Europe:

- **Strengthen Digital Services Act (DSA) enforcement** through anticipatory requirements for platforms on systemic risk mitigation and political advertising transparency, as well as guidelines for content moderation during election periods;
- **Operationalise the EUDS** as the EU's strategic infrastructure for real-time detection and rapid response to algorithmic manipulation, requiring and facilitating cooperation among Digital Services Coordinators (DSCs), regulators, civil society and trusted flaggers across borders and ensuring the capacity and independence of these bodies;
- **Establish additional dedicated coordination bodies** at national and regional levels (linked to the EUDS framework) to improve information sharing, pre-emptive monitoring and rapid crisis communication, as well as to facilitate adaptive research approaches;

- **Tighten campaign financing and improve advertising transparency** in line with the EU's forthcoming Regulation on the Transparency and Targeting of Political Advertising (TTPA), closing loopholes that enable the cross-border financing of online propaganda and disinformation;
- **Advance the enforcement of the European Media Freedom Act** (EMFA) to ensure full ownership transparency, disrupt disinformation financing networks and protect the independence of public-interest media;
- **Expand financial and in-kind support for credible media** to respond to emerging threats online, including to develop and implement training in positively impacting algorithmic spaces, maintaining audience trust and building societal resiliency via effective online communication;
- **Invest in digital literacy and "pre-bunking" initiatives, particularly among young and first-time voters,** to strengthen civic resilience against algorithmic disinformation and emotional manipulation online and to deter citizens from inadvertently abetting in their amplification;
- **Develop EU-backed, open-source digital forensics tools under the EUDS** to enable real-time media monitoring, cross-platform analysis and early identification of coordinated inauthentic behaviour that feed into adaptive research approaches; and
- **Build compliance with the EMFA, DSA and other relevant EU-level acts into accession criteria** for current and prospective candidate countries, especially in the Western Balkans, where media markets are most fragile and the security situation is particularly volatile, while also integrating these countries into the recommended cross-border monitoring and research initiatives.



Introduction

Romania's 2024-2025 presidential elections, which involved the cancellation of the first-round results at the end of 2024 due to allegations of Russian interference by Romanian intelligence, spotlighted the potential of foreign-backed influence operations to disrupt democracy. Romanian intelligence belatedly helped expose the ways that perpetrators of disinformation leverage social media algorithms to boost their reach online and tilt the electoral playing field in certain candidates' favour. The tactics identified fall under the umbrella of coordinated inauthentic behaviour, which, despite being defined differently by various social media platforms, generally refers to the practice of groups of fake accounts or pages linking up efforts to publish or promote content. [1]

Coordinated inauthentic behaviour and other forms of algorithmic manipulation are certainly not unique to TikTok, which was thrust into the spotlight after Romanian intelligence discovered that over 25,000 compromised accounts on the platform helped boost political newcomer Călin Goergescu to a stunning first-round victory. Other platforms like Facebook, Instagram and X were also implicated in the investigation and remain hotbeds for disinformation and potential information operations, as the other case studies in this report resoundingly show. In fact, this analysis indicates that perpetrators of these operations typically employ cross-platform strategies that can make it even more difficult to respond proactively and effectively.

Nevertheless, this report emphasises the role of information manipulation on TikTok given its algorithmic particularities, exponential growth of global users and mounting criticism that it responds far too slowly to allegations of platform abuse when they arise. In this sense, TikTok represents a unique vulnerability for European leaders to address.

While the Romanian presidential elections captured public attention, algorithmically-driven influence operations have attempted to skew recent elections across Europe and beyond, from Germany[2] to the United States.[3] Understanding the recurring tactics of algorithmic manipulation is therefore imperative, particularly in Europe's most fragile media environments like those of the Western Balkans. In this region, the tactics of manipulation unearthed in Romania are far from unique; rather, they pose a persistent threat to media markets already captured by party leaders and business actors and for polarised societies inundated with disinformation.

Allowing these kinds of influence operations to metastasise across the Balkans puts all of Europe at risk, as disinformation and election interference are fundamentally borderless. Moreover, the lessons learned from these countries' experiences on the "front lines" of such assaults to media freedom, democracy and security, will only become more essential to the European policy community. Perpetrators of algorithmically-driven influence operations are becoming increasingly sophisticated and geopolitical precarity and institutional distrust are beginning to look like the new status quo–not just in Southeastern Europe, but across Europe. In this moment, the impetus to act decisively could not be greater and this report aims to equip European leaders with the concrete tools to do so.

This introduction proceeds by providing additional background on TikTok's algorithmic design and its growth in the coverage region before detailing the report methodology. What follows the introduction are two, full-length case studies: one on Romania's 2024-2025 presidential elections and another on the snap elections in Bulgaria in June and October of 2024. The Romania chapter follows a timeline format to reconstruct the manipulation campaign in question and highlight possible mitigation strategies missed at various stages by relevant actors. The Bulgaria chapter is structured differently, starting with an overview of the particularities of the country's disinformation ecosystem before discussing non-TikTok and TikTok-specific vulnerabilities and mitigations. The report then offers a brief discussion of the case of Kosovo's parliamentary elections in February 2025, which saw similar manipulation tactics in a significantly more volatile security environment–a case study yet to be adequately explored by experts of algorithmic manipulation. It then concludes with an overview of findings and final recommendations.

[1] https://www.disinfo.eu/publications/cib-detection-tree-third-branch/#:~:text=INTRODUCTION,or%20coordinated%20and%20what%20not

[2] https://www.isdglobal.org/digital_dispatches/coordinated-disinformation-network-uses-ai-media-impersonation-to-target-german-election/

[3] https://cyber.fsi.stanford.edu/news/how-coordinated-inauthentic-behavior-continues-social-platforms

Platforms designed to reward coordination, not fight it

While the sheer volume and complexity of content make it difficult for social media platforms to detect influence operations and coordinated inauthentic behaviour specifically, the very architecture of these platforms rewards coordination rather than stops it.[4] Designed to maximise user engagement, the algorithms behind platforms analyse user interactions, video details and device settings to personalise content for viewers and keep them on the app as long as possible. This incentive structure, built around amplifying virality, creates two problems. First, it makes it technically difficult for platforms to detect coordinated content if it engages a large number of users. Second, this creates an inherent tension between platforms' commercial motives and disrupting popular–though potentially inauthentic and propagandistic–content.

The more the coordinated effort can utilise or successfully mimic genuine user behaviour, the harder it is for platforms to detect and combat the operation. Unsurprisingly, this is exactly what malicious online actors are getting better at doing. As the case studies in this report will show, algorithmic manipulation tactics have become more sophisticated than simple bot farms.[5] For example, the synchronised[6] use of trending hashtags[7] can be used to amplify specific narratives (including false narratives) and target specific geographic locations. If these narratives have local relevance, or if they are boosted by influencers and known figures, manufactured popularity[8] can become genuine popularity, making it even more difficult for platform algorithms to detect the coordination effort. Such tactics played an essential role in the Romanian, Bulgarian and Kosovan cases, as will be detailed in this report.

TikTok's meteoric rise in the Balkans and beyond

TikTok has transformed itself from a niche, short-form video application to one of the world's leading social media platforms. With 200 million monthly users in Europe alone[9], TikTok's user base officially reached a third of the continent's population in 2025 and its European advertising revenue surged 38% last year.[10] Romania and Bulgaria are among the EU member states with the highest rate of TikTok account penetration,[11] with almost half of their respective populations using the app–to the tune of millions of monthly users. Especially in Romania, which saw a 20% increase in its number of TikTok users going into 2024,[12] young people were early adopters of the platform, with about 65% of users in Romania being aged 18–24 as of May 2025. [13]

Because each platform's algorithm is proprietary, making each its own unique "blackbox," it is difficult to determine exactly what sets TikTok apart from other algorithmic-driven platforms like Facebook or X.[14] However, it appears that TikTok's algorithm is disproportionately influenced by individual user interactions, such as likes, shares and watch time.[15] Moreover, the high virality potential of short-form video content, due to its ability to evoke strong emotional responses from users, has also contributed to TikTok's potential to spread misleading information.[16]

[5] https://www.wsj.com/podcasts/tech-news-briefing/how-does-tiktok-algorithm-know-you-so-well/628ed5a0-e070-4653-b7ce-f49f6aeb1e17#:~:text=And%20so%20the%20Wall%20Street%20Journal%20and,the%20app%20works%20or%20the%20algorithm%20works

[6] https://arxiv.org/html/2505.10867v1#:~:text=As%20a%20result%2C%20a%20coordinated,%F0%9D%95%8F%20%2C%20Facebook%2C%20and%20Telegram

[7] https://www.researchgate.net/publication/382423048_Understanding_the_Impact_of_TikTok's_Recommendation_Algorithm_on_User_Engagement#:~:text=2.5.,high%20engagement%20rates

[8] https://brodhub.eu/en/romanian-elections-2025/analysis-of-social-media-presence-of-romanian-presidential-candidates-2nd-edition/

[9] https://www.socialmediatoday.com/news/tiktok-reaches-200-million-users-in-eu-europe/759454/

[10] https://www.thekeyword.co/news/tiktok-europe-revenue-grows-38-to-6-3b-in-2024

[11] https://datareportal.com/reports

[12] https://www.romania-insider.com/romania-youth-digital-skills-tiktok-adoption-2024

[13] https://www.reuters.com/world/europe/romanian-voters-again-turn-tiktok-guidance-rerun-annulled-election-2025-05-01/

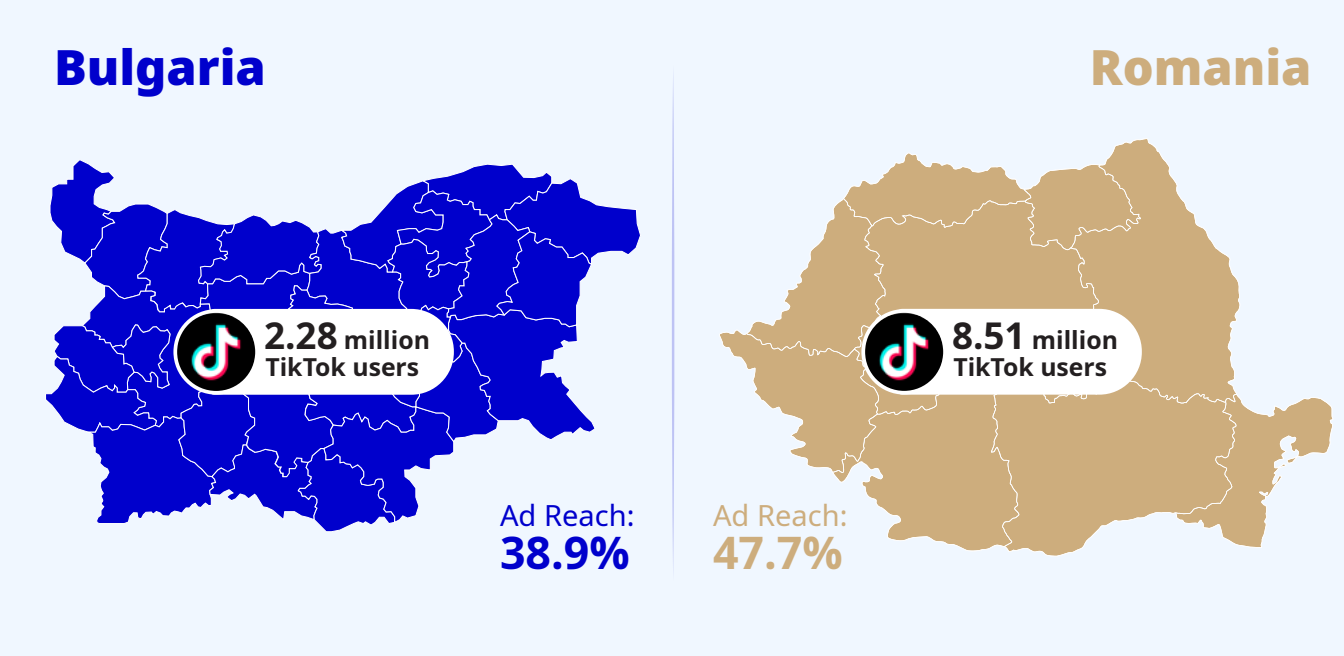
[14] https://www.internationalaffairs.org.au/australianoutlook/deceptive-trends-the-societal-impact-of-disinformation-on-tiktok/

[15] https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html#:~:text=The%20document%2C%20headed%20%E2%80%9CTikTok%20Algo,so%20hard%20to%20put%20down

[16] https://arxiv.org/html/2506.05868v1#:~:text=Research%20on%20online%20coordinated%20behaviour,highlighting%20potential%20pitfalls%20and%20limitations

TikTok's evident failure to spot inauthentic or coordinated behaviour is all the more worrying given that other platforms now spotlight short-from content and are increasingly mimicking TikTok's interface[17] and its algorithmic design.[18] Finally, it is worth noting that there is circumstantial evidence to suggest that the Chinese owners of the algorithm have been modifying it for political aims,[19] though this may change under the proposed American ownership.[20]

TikTok's Reach in Bulgaria and Romania



Methodological introduction

The Romania chapter of this report utilizes desk research and data collected by local civic organisations in the country during the relevant election periods. Though this data has been publicly available for some time, few reports have consolidated this data into a single, coherent narrative that outlines, step by step, the nature of Georgescu's manipulation operation and the various mitigation strategies that could have prevented its reach. The strategies throughout this report are derived from additional desk research and informal conversations with relevant experts, representing a unique contribution to the development of European policy on these critical topics.

However, the research on Bulgaria and Kosovo is heavily influenced by a unique data set collected by this report's technical partner, Sensika. Sensika's novel approach to data collection and analysis allowed the report authors to detect artificially boosted or coordinated political content on TikTok at a high scale and over designated periods of time before and after the election dates.

This methodology combines quantitative data analysis and deep network mapping to distinguish organic user engagement from inauthentic or manipulated activity. This was complimented by qualitative and textual analysis of relevant TikTok videos to better understand drivers of video virality regardless of whether the content was inauthentically or authentically boosted.

The analysis began by identifying networks of accounts amplifying political messages. Researchers started from key political hashtags and traced which accounts appeared most frequently, how often the same videos were reposted or stitched and whether these activities extended to other platforms such as Facebook,

[17] *https://www.linkedin.com/pulse/why-all-social-media-aiming-mimic-tiktoks-success-moldir-nurpeissova/*
[18] *https://www.bbc.co.uk/news/articles/cmm3yn4pr17o*
[19] *https://samf.substack.com/p/three-seconds*
[20] *https://edition.cnn.com/2025/09/22/tech/tiktok-sale-oracle-algorithm#:~:text=The%20White%20House%20has%20answered,States%20and%20overseen%20by%20Oracle*

Instagram or Telegram. Each TikTok video was then assessed for indicators of manipulation using several measurable criteria, cross-checked against TikTok's own policy framework, which prohibits fake views, likes and coordinated inauthentic behaviour. These indicators included:

- Low engagement rate: Videos with large numbers of views but disproportionately few likes, comments, or shares were treated as potential signs of artificial boosting. Benchmark data suggest that normal engagement on TikTok is above 3%, while content falling below 2%—and especially below 1%—is highly suspicious.
- Metric imbalances: Unnatural ratios, such as many likes but almost no comments or shares, or sudden spikes in followers, were flagged as indicators of purchased engagement or automated activity.
- Repetitive posting and commenting ("Fire Hose" pattern): Identical or near-identical videos and comments posted by multiple accounts within short intervals indicate attempts to overwhelm TikTok's algorithm and generate artificial visibility.

Videos meeting multiple red-flag criteria—such as low engagement rates combined with repetitive posting or metric inconsistencies—were classified as suspicious or likely manipulated. Sensika's blended methodology is in and of itself a contribution to this field of analysis, offering an evidence-based foundation for researchers and policymakers to better understand how manipulation occurs within TikTok's recommendation systems.

Combined with qualitative analysis of the content itself, this approach also allowed researchers to draw out lessons about effective online communication outside the bounds of algorithmically or partially boosted content. This research process underscores that measures against inauthentic content are legitimate and sorely needed in defence of democracy, as the following chapters will confirm. Yet it also suggests that "successful" or genuinely-popular content by non-democratic actors requires a systematic, democratic response in the form of open, creative and innovative communication and technical adaptation by media and political actors alike.

Democracy, trust and security on the line

Election-related influence operations like the ones documented in this report have immediate political ramifications and pose urgent security threats. These operations have the potential to sway public opinion at critical moments and open countries up to foreign interference. Particularly pernicious is the non-transparent financing undergirding these disinformation networks, as it puts societies at risk of money laundering and corruption while, at the same time, hurting genuine media competition. This constantly puts independent media "on the backfoot," undermining its ability to provide credible reporting, foster open debate and build relationships of trust with audiences–all essential to combating these operations in both real time and in the long-run.

As such, these influence operations can also have lasting negative effects on democracy, security and prosperity. By damaging the public's trust in political institutions, these operations delegitimise the democratic project. And, by subverting media freedom to serve private interests rather than the public good, they rob citizens of a critical tool for accountability and activism. Polarised, distrustful societies without institutional mediation mechanisms not only lose their resiliency, they are also at greater risk of conflict.

In the Balkans, a post-conflict region already deeply polarised and with an entrenched legacy of media capture, influence operations that rely on algorithmic manipulation have a disproportionate impact on democracy and security. When media markets are highly concentrated, with overlapping ownership structures and tight links between business and politics, it is all too easy for disinformation from fake websites or social media to bleed into mainstream media. As narratives gain traction–especially through artificial boosting on platforms–the noise becomes

[21] *See Appendix I for Sensika's methodology.*

[22] *https://dfrlab.org/2024/03/26/suspicious-facebook-assets-bulgarian-mushroom-websites/*

[23] *https://dfrlab.org/2024/03/26/suspicious-facebook-assets-bulgarian-mushroom-websites/*

difficult to contain outside credible media. Once this content makes its way into traditional media channels, not only is its reach extended but its narratives are also legitimised. This spillover effect damages the credibility of independent media and other democratic institutions while also amplifying divisive tropes, feeding polarisation and fomenting conflict.

Foreign actors have taken advantage of anti-democratic disillusionment in this region, as well as glaring regulatory gaps, in order to mount a wider assault on the continent's information system and Europe's very values. As the Balkans increasingly become a testing ground for algorithmic influence operations by Russia and by home-grown political actors, it is also becoming one of Europe's greatest vulnerabilities. This report aims to provide European leaders with a roadmap for preventing and combating such influence operations in both EU and non-EU contexts based on recent case studies from this critical region.

The report also envisions a central role for credible media, one that is integrated in the broader disinformation-fighting ecosystem outlined therein. Despite the growing crisis of trust in traditional media, independent outlets and journalists still play a central role in educating citizens and facilitating truth-based democratic debate. New mechanisms of support, whether financial or in-kind, are needed to ensure that the media sector transforms in tandem with Europe's regulatory environment and technical capacities. Ultimately, the report makes the case that traditional and "new media" must be deployed together in the envisioned democratic defence plan.

The following summary table of this report's recommendations demonstrates the highly interlinked and interdependent nature of the measures required to reimagine Europe's democratic defence. In the report's conclusion, we will present these same recommendations categorised by the relevant actors and organisations that will be needed to fully implement the proposed blueprint. While each recommendation is detailed fully in callout boxes throughout country-specific chapters, the report authors wish to emphasize that all identified recommendations are applicable in each case study and across Europe more broadly.

Summary of recommendations thematically

Societal	Regulatory	Institutional	Technical
Public awareness campaigns, media / digital literacy campaigns. "Whole-of-society" approach / consultative mechanisms for civic actors, media professionals and fact checkers, technical experts, private sector representatives etc.	Enforcement of DSA - EC sets clear guidelines for platforms on "systematic risk mitigation" - EC sets guidelines for non-VLOPs like Telegram - EC creates designated teams under DG CONNECT tasked with consistent platform accountability enforcement Tighter campaign financing rules + stronger election bodies to enforce. Tighter political advertising regulation, including enforcement of forthcoming TTPA. Stronger enforcement of ownership transparency obligations such those under the EMFA.	Inter-institutional / cross-sectoral action plan prior to elections + escalatory protocols when manipulation is detected. Establishment of a leading agency / centralised StratCom body / bodies to proactively monitor information space. These bodies must account for local realities and may require varying levels of centralisation and coordination to avoid possible politicisation or capture. Clear and transparent content / account removal guidelines + early deployment of trusted "local flaggers," i.e. local civic monitors. Revamped financing and in-kind support for independent media specifically targeting areas of digital transformation, effective online communication and disinformation-fighting capabilities.	Digital forensics tool kit, including media monitoring and audience analysis tools, that will allow a dedicated, cross-functional task force to track and investigate manipulation in real time. An open-source investigative platform to house these forensic tools and allow for the future development of machine learning and algorithmic solutions for spotting information operations as well as more adaptive research initiatives more generally. Financial forensics that combine anti-money laundering best practices with targeted actions against the advertising supply chain that fund disinformation sites.

[24] *https://www.pew.org/en/trend/archive/fall-2024/media-mistrust-has-been-growing-for-decades-does-it-matter*

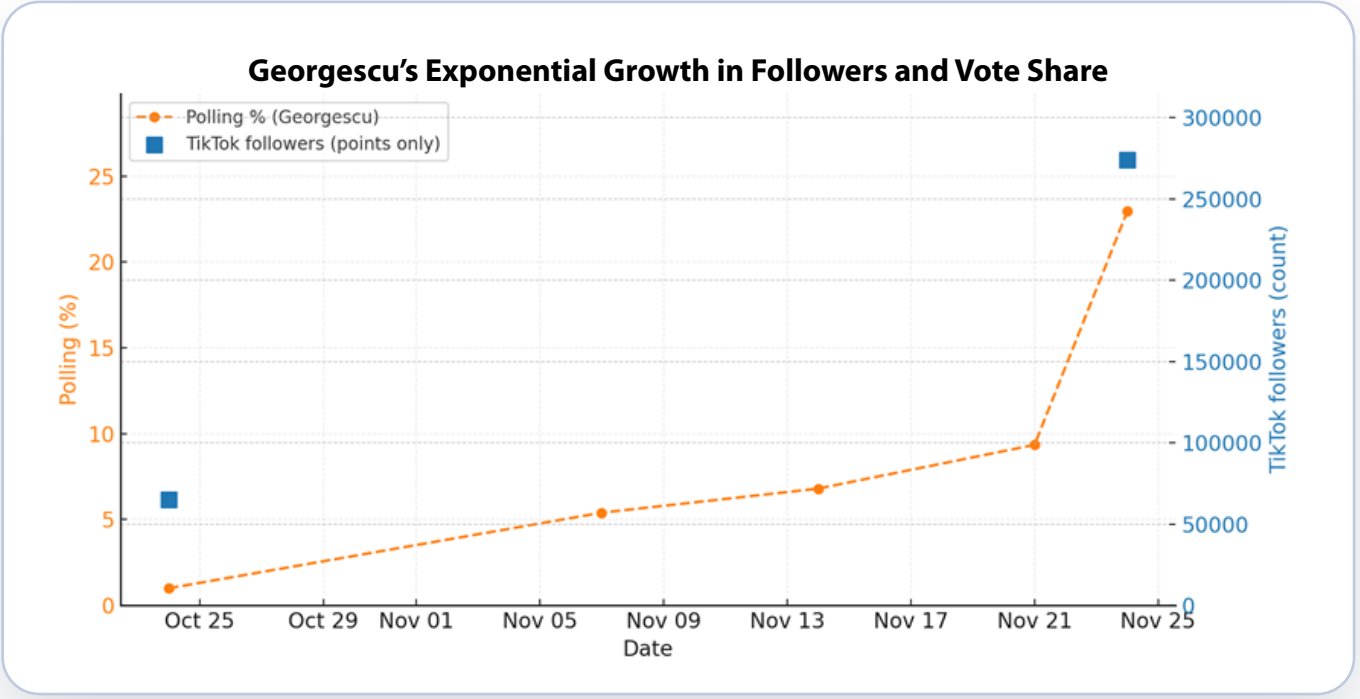
Romania

Romania's presidential election took place on November 24, 2024. The political establishment and the Romanian public were shocked when Călin Georgescu, an independent candidate and relatively unknown figure with pro-Russian views, won the first round that day. As no candidate achieved an absolute majority, a second round had been scheduled for December 8. Voting had already begun in polling stations abroad when, on December 6, Romania's Constitutional Court annulled the election, alleging that Romanian intelligence had uncovered a Russian influence operation that had impacted the vote and propelled Georgescu to victory.

Authorities later scheduled the presidential election rerun for spring 2025, with the first round held on May 4, 2025. In March, authorities barred Georgescu from running, paving the way for a wide range of candidates to compete for the second round on May [18]. Ultimately, George Simion of the far-right Alliance for the Union of Romanians (AUR) party faced pro-European independent Nicușor Dan. The contest was widely interpreted as a watershed moment for the future of Romanian democracy and the country's orientation toward Europe. Despite coming in second place during the first round, Dan ultimately won the election on May 18 with about 53.60% of the vote over Simion's 46%.

Although international media painted Dan's win as a victory for Romanian democracy, questions about the Constitutional Court's decision to annul the initial results from 2024 remain. Likewise, political and technical experts are still making sense of Georgescu's manipulation operation and the extent of Russian involvement in the confirmed influence operation, which mainly operated on TikTok according to Romanian intelligence and local civic groups.

This chapter details the evolution of Georgescu's information operation, detailing the main actors and tactics essential to its success in boosting him from obscurity to victory. In doing so, the chapter identifies societal, regulatory, institutional and technical recommendations that could have mitigated against Georgescu's manipulation operation and can prevent future large-scale acts of algorithmic manipulation on TikTok and other platforms.



[25] https://www.robert-schuman.eu/en/monitor/6566-nicusor-dan-wins-the-presidential-election-in-romania

Overview of tactics behind Georgescu's operation

In the lead up to the November presidential election race, Georgescu's coordinated online campaign utilised two main tactics simultaneously in order to reach potential voters: 1) generating targeted content and 2) inflating user engagement metrics via automated accounts and paid promotions. This hybrid approach saturated the platform with favourable messaging by taking advantage of TikTok's algorithm, while also avoiding detection by the platform.

At the same time, the local relevance of the content allowed Georgescu to convert this manufactured popularity into "genuine" or organic reach, creating a highly effective cycle of online engagement that evidently led to voter conversion. Georgescu not only amassed 646,000 followers and 7.2 million likes on TikTok in the two months before the election; he also skyrocketed from political obscurity to the top of the polls, with 22.94% of the vote on election day.

Before the presidential re-run in May, national authorities pushed through new regulations concerning online campaign violations and TikTok built out a local response team to monitor and remove suspicious accounts and activity. Despite these efforts, monitoring by local civic groups suggests that coordinated inauthentic behaviour continued to proliferate via official candidate accounts on TikTok and other platforms, though on a much smaller scale.

Analysis: operation timeline & missed mitigation strategies

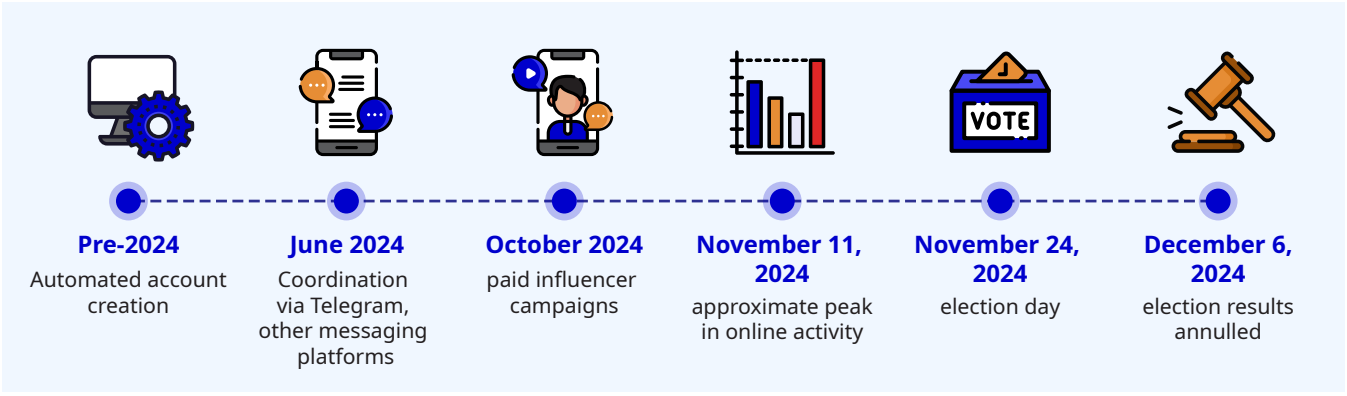
The following analysis documents how presidential candidate Călin Georgescu's TikTok campaign evolved over time, from well before the start of the electoral period, through election day, the decision to repeat the race and the final results in May 2025. This section then identifies possible mitigation strategies missed by national authorities, platforms and European institutions that could have helped prevent or mitigate the full effects of this operation.

National authorities missed opportunities to warn the public about the risks of online news consumption during the electoral period; mount a proactive, effective, transparent and inter-institutional response; and adjust electoral rules to prevent or adequately monitor political advertising and campaign finance violations. Meanwhile, European institutions failed to set clear guidelines for platforms to meet their risk mitigation obligations under the newly in force Digital Services act (DSA), ultimately leading TikTok to respond reactively, in an over-handed manner that hurt civic activism and public debate during a particularly sensitive political moment.

As such, the recommendations noted in the following analysis mainly address these regulatory, institutional and societal vulnerabilities, with some specialised recommendations aimed at addressing the technical aspects of Georgescu's operation.

[26] *https://apnews.com/article/who-is-calin-georgescu-romania-e768e118f8adc84ff2f8a38e30439b78*

Overview of Georgescu's manipulation operation



Before 2024: automated account creation

Declassified documents from Romanian intelligence indicate that over 25,000 automated TikTok accounts were used in Georgescu's operation, created in large batches between 2016 and 2023. Only a small number of those accounts, nearly 800, date back to 2016. The bulk of the account creation took place between 2022 and 2023 and amounted to over 20,000 accounts. Most were "sleeper accounts," inactive or minimally active upon their creation, though some did start to build small audiences in the years prior to the 2024 presidential election.

Additional investigations found that many of these accounts were registered with recycled phone numbers and emails, suggesting that they were likely created using bot farm techniques associated with prior Russian information operations. Romanian intelligence services also reported that IP data and server activity from many of the fake accounts matched Russian infrastructure. However, local Romanian intermediaries must have reactivated those accounts.

Missed Mitigation Strategy: Public awareness campaigns and digital literacy campaigns supported by European and national authorities and implemented by civic educators

In the leadup to the 2024 presidential elections, Romanian experts decried the public's lack of awareness of the risks of online disinformation, blaming the government's poor public communication[31] around these topics, low media and digital literacy rates[32] among citizens and a generalised atmosphere of institutional distrust[33] following years of ineffective governance.[34] These issues were only exacerbated with the eventual annulment of the election results, as authorities failed to adequately explain the decision to the public.

Had Romanian and/or European authorities invested in public awareness campaigns prior to the race about the risks of information manipulation, similar to the efforts by Moldova[35] in the leadup to the 2025 parliamentary elections there, Romanian citizens may have been better prepared to encounter inauthentic or coordinated behaviour online. Moreover, had Romanian and/or European authorities invested in educational initiatives aimed at enhancing literacy and resiliency, young voters in particular may not have been as vulnerable to the disinformation narratives linked to Georgescu's manipulation operation, nor would citizens have been as likely to inadvertently amplify Georgescu's content further.

TikTok did work with local civic groups in the leadup to the 2025 rerun to create and promote videos[36] aimed at empowering users with tools to critically evaluate online content and access credible information. Had such an initiative been planned in advance of the initial races in 2024, citizens may have been better equipped at that time.

[27] *https://www.romaniajournal.ro/politics/iohannis-declassifies-documents-in-csat-meeting-revealing-operation-of-a-state-actor-to-promote-calin-georgescu/*
[28] *https://vsquare.org/step-by-step-through-calin-georgescus-tiktok-campaign-playbook/*
[29] *https://www.ft.com/content/4b00e7ec-2c79-4313-b012-4f09f436f3ed*
[30] *https://www.romaniajournal.ro/politics/iohannis-declassifies-documents-in-csat-meeting-revealing-operation-of-a-state-actor-to-promote-calin-georgescu/*

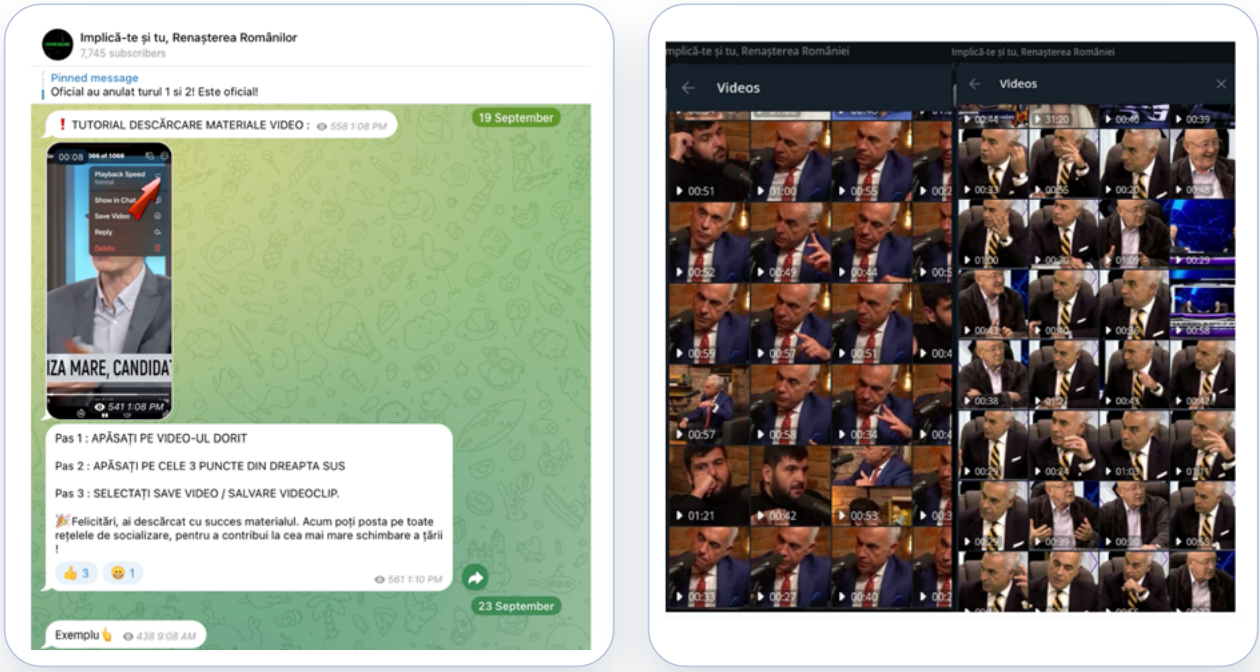
Missed Mitigation Strategy: Clear and effective European Commission guidelines for DSA implementation

While the onus is not solely on platforms to combat coordinated and inauthentic behaviour on their channels, they naturally play a significant role in preventing it. The European Commission must do more to steer platforms in the implementation of the DSA. Had the Commission set clear and specific guidelines or best practices for the implementation of Articles 34, 35 and 37 of the DSA (but especially 35.3)[37]regarding "reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks," rather than leaving these areas solely to the platforms to define and implement, TikTok may have been incentivized to develop a more robust set of prevention measures in advance of the Romanian elections, rather than turning to reactive measures later on, such as content and account removal that posed risks to civic activism and free speech. Concretely, the Commission should consider specifying detection, labelling and transparency expectations related to these and other articles.

Moreover, the European Commission could also consider expanding some DSA requirements related to "systemic risk" factors, such as mandating more frequent risk assessments and requiring these assessments be vetted by independent experts. It could also consider defining clear metrics (e.g., volume of removed inauthentic accounts, average response time, transparency on takedowns) for platforms to track and disclose as a measure of performance from cycle to cycle, which would shift platforms' focus from one-off actions to continuous engagement and provide a level of self-imposed accountability.

6 months before election day: Telegram coordination

A Telegram channel named Propagator (linked to a TikTok account called @propagatorcg that was created on June 15, 2024[38]) appears to have been made with the sole purpose of coordinating the promotion of Georgescu on TikTok and other platforms. Another 76 TikTok accounts were created from this group. Throughout the summer, similar Telegram channels serving the same coordination purpose popped up across the country.[39] These channels had up to thousands of members at one time, with moderators sharing images and videos with explicit instructions on how to edit, personalise and share the content across platforms. This coordination effort allowed for a constant stream of user-generated content to be deployed on TikTok and other platforms and be boosted by the large network of automated accounts already created.



Screenshots of a Telegram group (left) used to coordinate the sharing of pre-edited videos (right). Source: DFRLAB.

[38]*https://www.romaniajournal.ro/politics/iohannis-declassifies-documents-in-csat-meeting-revealing-operation-of-a-state-actor-to-promote-calin-georgescu/*

[39]*https://edmo.eu/wp-content/uploads/2025/03/BROD_Elections_M_Botan-compressed.pdf*

Missed Mitigation Strategy: Expanded DSA risk mitigation obligations for other social media platforms prior to election day

Telegram is increasingly becoming a hub for disinformation and coordinated information operations, as it is one of the few messenger applications which has broadcast channels that other users can follow. Another gap in the implementation of the DSA that the European Commission must address is relevant risk mitigation by platforms not designated as "Very Large Online Platforms" (VLOPs) like Telegram. Had Telegram been subject to the same or similar risk management obligations as VLOPs like TikTok, the possibility of widespread coordination well before the election could have been mitigated.[41]

Missed Mitigation Strategy: Inter-institutional and cross-sector action plan against election-related information manipulation

National authorities have commitments under the DSA to formulate an institutional response to information manipulation like that documented in Romania's 2024 elections. In the Romanian case, the lack of inter-institutional collaboration was one of the main driving factors behind the slow and ineffective reaction by national authorities. Local civic groups describe "turf wars" between key institutions.[42]Had Romanian authorities resolved these inter-agency disputes in advance and developed an action plan outlining clear mandates, roles and responsibilities for each body, preparation for the election, monitoring of the online environment and the reaction to any online manipulation would have been more effective.

The lack of institutional collaboration only exacerbated criticisms of non-transparency by government actors and the platform after the first-round results were annulled, especially by Romanian civic actors that have a key role to play in fighting against information manipulation.[43]The involvement of civic actors, representatives from the platforms, other private sector actors, media professionals and educators would have constituted an effective "whole-of-society" approach, which would have created preparedness across sectors, facilitated critical data sharing as part of the election monitoring effort and laid the groundwork for escalatory procedures. A dedicated agency to lead such an effort and proactively monitor its implementation would also have created community cohesion–possibly improving public trust in authorities' response. The European Commission has a role to play in compelling national governments and platforms to participate in this aspect of DSA implementation, convening actors across sectors where applicable and ensuring that transparent consultative mechanisms are respected.

1 month before election day: paid promotions

Using influencer marketplaces such as Romanian startup FameUp and a marketing agency registered in South Africa, FA Agency, hundreds of influencers with small audiences of 10,000-50,000 followers were paid to upload promotional videos on Georgescu's behalf. One of the leading financiers identified by intelligence, Romanian programmer Bogdan Peșchir, sent payments to influencers from October 24 through election day on November 24, 2024.[44] Influencers received the funds through these agencies via virtual wallets, helping the effort go undetected. Peșchir also allegedly paid nearly a million euros to influencers by sending them TikTok "gifts," online tokens worth real money, from his account, "bogpr," in another means of avoiding detection.[45]

[42]*https://expertforum.ro/en/2024-romanias-struggle-with-systemic-risks-in-digital-services-act-implementation/#:~:text=Challenges%20in%20Implementing%20the%20DSA,the%20extent%20of%20institutional%20weaknesses*
[43]*https://expertforum.ro/en/data-access-election-integrity-lessons-from-online-disruptions/*
[44]*https://agerpres.ro/2024/12/04/declassified-documents-from-csat-romania---target-of-russian-hybrid-actions-georgescu-s-campaign---f--1398576*
[45]*https://www.bbc.co.uk/articles/cqx41x3gn5zo*

Missed Mitigation Strategy: Air-tight campaign financing rules developed and implemented by national authorities with multi-sector consultation

Reporting on campaign expenditures is only required of parties and officials during election periods in Romania. The current requirements do not go far enough in cataloguing exact expenditures, especially as candidates and parties use consultancy agreements and digital payment systems to hide spending, as was clear in the case of Georgescu's manipulation operation but which is also a widespread election practice, according to the OSCE/ODIHR.[46]

According to Romanian civic groups, the January emergency ordinance put in place new processes and stricter deadlines for adjudicating disputes related to online campaign violations.[47] It did not, however, address fundamental campaign financing issues such as the large size of subsidies received by parties to fund campaign materials (especially in second-round races[48], the flawed process of verifying campaign expenses and the lack of interim financial reporting requirements. Had such measures been in place prior to the 2024 election, authorities would have had more effective tools for investigating use of funds. In the future, Romanian authorities should consider implementing mechanisms for the real-time detection of funds flow. Recommendations by the Financial Action Task Force (FATF) to detect and deter fraudulent online payments should also be considered,[49] as such measures could have potentially limited payments made by Georgescu's financiers via FameUp or TikToK.

Missed Mitigation Strategy: Effective, efficient and transparent election bodies with stronger mandates to investigate and sanction financial misdeeds

The Permanent Electoral Authority is one of the main bodies mandated to administer elections in Romania alongside a three-tier structure of election bureaus. OSCE/ODIHR has recommended in past election reports that the mandate of this body be enhanced to allow for more effective identification of and stronger response to campaign finance irregularities, including expanded auditing and sanctioning powers. Had there been tighter campaign finance regulation as well as a more transparent, higher-capacity body to monitor and react to irregularities prior to the 2024 elections, the response to reports of paid-for inauthentic coordination may have been more proactive and effective.

The EUDS has the potential to bolster strengthened electoral bodies through the projected technical and operational support, as well as through the cross-border harmonisation and collaboration envisioned under the European Cooperation Network on Elections (ECNE). Practically, this could include facilitating capacity-building initiatives, sharing EU-wide analytical tools and best practices and offering training in financial auditing and digital transparency measures. Such initiatives would legitimise the enhancement of auditing and sanctioning powers while embedding them in a broader European effort to promote stronger election standards and safeguard from interference.

The influencers were provided with pre-written scripts to follow and told which hashtags to include on the videos.[51] In some cases, posting schedules were synchronised to maximize reach. Many of these influencers claimed that they did not realise what they were being paid to do. Some did not even mark their posts as paid promotional content, thinking that they were participating in an apolitical "get out to vote" campaign. Nevertheless, they later described how their videos went viral almost immediately upon posting, thanks to a flood of comments–presumably from the automated account network created prior to the campaign. [52]

TikTok failed to detect this content as political advertising, which is banned on the platform. While some influencers may have violated local law, legal liability at the time of Georgescu's manipulation operation at the end of 2024 was still vague and untested, failing to provide any deterrence.

[46] *https://www.osce.org/files/f/documents/d/9/576663.pdf*
[47] *https://www.g4media.ro/zece-ong-uri-despre-ordonanta-de-urgenta-cu-sanctiuni-pentru-social-media-care-favorizeaza-un-candidat-modifi-carea-legii-electorale-trebuie-facuta-transparent-si-fara-a-afecta-drepturile-fundamental.html*
[48] *https://www.osce.org/files/f/documents/d/8/590963.pdf*
[49] *https://www.fatf-gafi.org/en/topics/fatf-recommendations.html*
[50] *https://www.osce.org/files/f/documents/d/9/576663.pdf*
[51] *https://hotnews.ro/calin-georgescu-urmele-banilor-un-influencer-de-pe-tiktok-recunoaste-ca-a-fost-platit-pentru-campanie-1845987*
[52] *https://www.bbc.co.uk/articles/cqx41x3gn5zo*

Missed Mitigation Strategy: Measures for political advertising transparency by authorities and platforms

Romanian authorities in January moved quickly to rectify the lack of labelling of paid content and other persistent issues around political advertising, such as by requiring campaign materials to be clearly marked and sponsors identified via a system of unique coding. Had these restrictions been in place before the 2024 elections, Georgescu's manipulation operation would likely not have had the reach that it did, as his ability to use influencer and supporter networks would have been appropriately curtailed. Moreover, Romanian authorities would have been able to proactively communicate to influencers and the public about the risks of participating in such campaigns, while also deterring these activities with real-time exemplary actions against transgressors.

The January measures generally aligned with the EU's Regulation on the Transparency and Targeting of Political Advertising (TTPA), which came into full effect in October 2025.[55]However, the rushed nature of the changes and lack of consultation led to transparency and possible censorship concerns by civil society.[56]These concerns could have been alleviated had authorities made such regulatory changes well before the election and after a refined consultation process with civil society organisations..

While TikTok prohibits political advertising, numerous global investigations show its enforcement of this prohibition is extremely weak.[57] Platforms must update both their policies and enforcement process related to political advertising, including developing easy and effective tools for creators to self-disclose paid or sponsored content. Some platforms are taking such steps–and investing in stronger advertising transparency in general–in anticipation of the TTPA's application at the end of 2025.[58] TikTok appears to be moving slowly in this effort while it is still under investigation by the European Commission for its failure to detect political advertising in the Romanian case as well as for other possible DSA breaches.[59] In the future, expedited investigations by the Commission could help spur more rapid action from platforms as well.

2 weeks before the election: peak online activity

Georgescu's network of automated accounts was activated and/or reactivated in the two weeks before the election, starting on or around November 10-11, 2024. This large network began to amplify pro-Georgescu content, and, as a result, this period was the peak of inauthentic coordinated behaviour and a period of exponential growth in Georgescu's online following.

This network of accounts posted thousands of videos promoting Georgescu directly and/or spread narratives favourable to his campaign, including mis- and disinformation. The accounts also flooded the comments of unrelated videos with pro-Georgescu comments at peak engagement times. These comments included the use of strategic hashtags such as #calingeorgescu, #prezidentiale2024 and #echilibrusiverticalitate, gaining millions of impressions. This mass posting and "comment bombing" strategies, thanks to TikTok's algorithm, got Georgescu's name trending and pushed both his official account and other pro-Georgescu content to more users. Much of the content was user-generated from supporter channels and paid influencers, allowing the online campaign to appear authentic and avoid detection by the platforms. This approach also helped Georgescu reach niche audiences across the country, generating genuine support from the manufactured user reach afforded by his network of 25,000 automated accounts.

[53]*https://www.reuters.com/world/europe/romania-confirms-date-tightens-rules-presidential-election-rerun-2025-01-16/*

[54]*https://cmpf.eui.eu/country/romania/#:~:text=There%20were%20a%20few%20regulatory,content%20sponsored%20by%20party%20x%E2%80%9D*

[55]*https://www.consilium.europa.eu/en/press/press-releases/2024/03/11/eu-introduces-new-rules-on-transparency-and-targeting-of-political-advertising/#:~:text=Political%20advertisements%20must%20be%20made,cannot%20be%20used%20for%20profiling.*

[56]*https://www.politico.eu/article/romania-online-censorship-presidential-election-social-media-russian-interference/#:~:text=French%20political%20crisis-,Romanian%20government%20accused%20of%20online%20censorship%20ahead%20of%20election%20rerun,Simion%20are%20among%20those%20targeted.*

[57]*https://www.mozillafoundation.org/en/campaigns/tiktok-political-ads/recommendations/*

[58]*https://www.aljazeera.com/economy/2025/7/25/meta-to-suspend-political-advertising-in-the-eu-as-transparency-law-looms*

[59]*https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1223*

[60]*https://funky.ong/wp-content/uploads/2024/12/RaportAlegeri2024.pdf*

[61]*https://edmo.eu/wp-content/uploads/2025/03/BROD_Elections_M_Botan-compressed.pdf*

Missed Mitigation Strategy: Establishment of a centralised strategic communications body by national authorities to proactively monitor information space, branded as a Democracy Defence Commission or similar

The absence of a centralised Strategic Communications (StratCom) body in Romania left opaque intelligence services to lead in the monitoring and response efforts, which not only proved ineffective but also left citizens without oversight of these critical processes for their democracy.[62] Numerous government agencies also claimed to be monitoring the online environment but evidently failed to either detect or report Georgescu's efforts. Had Romania followed the model of countries that have dedicated agencies with such a mandate (such as Poland[63] and Moldova[64]), the possibility of detecting Georgescu's manipulation operation would have been more likely. Moreover, the national response to findings of coordinated inauthentic behaviour could have been more proactive and effective. Branding such a body as a "Democracy Defence Commission" or similar would provide mandate clarity to the public and support society-wide communication and education efforts, which could also fall within the direct mandate of this institution depending on its structure.

While Georgescu's operation leveraged sophisticated coordination efforts, an essential aspect of the campaign's success was the emotional appeal and local relevance of the narratives disseminated, including how content was tailored to reach key demographics like young people, the Romanian diaspora and other dissatisfied citizens. Using targeted, locally-grounded content allowed Georgescu to convert genuine support from algorithmically-manufactured popularity–a lesson that both policy makers and traditional media would do well to heed.

Some of the main themes in the content promoted on Georgescu's official account and through his coordinated campaign included anti-Western messaging such as anti-EU and anti-NATO narratives, as well populist and nationalist ideas about Romania's "threatened" sovereignty.[65] Short, emotional appeals–which do especially well on TikTok's algorithm–framed Brussels as exploitative and corrupt, with the goal of subjugating and robbing Romanians. NATO was fashioned as the embodiment of American imperialism, risking dragging Romania into conflicts outside the country.

Many of these points echoed latent cultural and historic pro-Russian sympathies in the country[66], but the content was not explicitly pro-Russia, as this would not have resonated with most Romanians, who did not have especially positive views of Russia.[67] Instead, the most effective narratives were ones that discredited mainstream parties and Romanian institutions for being part of a dishonest and "rigged" system that put "ordinary Romanians" at risk of violence or deprivation.[68]

A screenshot of one of Georgescu's most popular videos on TikTok, which falsely claimed that Ukrainian refugee children receive more government assistance than Romanian children. Source: RFE/RL

[65] https://edmo.eu/publications/undermining-democracy-the-weaponization-of-social-media-in-romania%CA%BCs-2024-elections/
[66] https://www.politico.eu/article/romanias-presidential-frontrunner-benefited-from-russia-style-booster-campaign-declassified-docs-say
[67] https://www.globsec.org/what-we-do/publications/public-attitudes-romania-staying-west-some-doubts
[68] https://www.ft.com/content/37347819-22ba-4b6d-a815-ec6115a8f5af

Given Romania's poor democratic and economic track record over the last few years, it is no surprise that these messages gained real-life traction after being artificially boosted to millions of Romanian TikTok users, many of whom are young and disenchanted with the status quo in their country. Not only did TikTok's short-form video content take well to these kinds of narratives but memes and viral trends were also well suited to Georgescu's "anti-system" politics and helped with reach. Again, such communication strategies can–and should–be adapted by pro-democratic actors when possible.

Screenshot taken by the report authors of a GIF uploaded to Tenor, a common GIF library, on December 12, 2024.

Missed Mitigation Strategy: Clear and effective guidelines for content moderation and removal balanced with freedom of speech concerns and backed by appropriate platform compliance measures

TikTok's criteria for the removal of posts and accounts from the platform have long faced criticism for their lack of transparency. The platform and Romanian authorities faced additional scrutiny when the Central Election Bureau enacted a governmental emergency ordinance, which ordered the removal of posts designated as unlawful within 5 hours of flagging or risk fines between 1-5% of the related revenue.[72] Had Romanian authorities reached out to TikTok and other platforms to develop content and account removal guidelines in advance of the election–and with intentional consultation from civic society, media and technical experts–robust and transparent guidelines could have been created for moderation and removal. Such institutional accountability would have also facilitated greater trust among platform users and citizens and avoided potential freedom of speech violations.

Rather than issuing heavy-handed fines with short reaction timeframes to TikTok and other platforms, which led to much broader removals than may have been appropriate, authorities should have consulted with technical experts and the private sector and socialised the proposed penalties with the European Commission for a strengthened compliance architecture. In the future, Romanian authorities should coordinate enforcement through its DSC and rely on the DSA's mechanisms for imposing penalties, including against entities registered outside Romania.

[69] *https://freedomhouse.org/country/romania*

[70] *https://www.romaniacurata.ro/servicii-publice-locale/en/2023/10/05/the-2024-elections-through-the-eyes-of-young-people/*

[71] *https://brodhub.eu/en/romanian-elections-2025/analysis-of-social-media-presence-of-romanian-presidential-candidates-2nd-edition/*

Missed Mitigation Strategy: Early deployment of "trusted flaggers"

The data from the Romanian case shows a peak in coordinated inauthentic behaviour in the two weeks leading up to election day. It was only after the results were annulled that TikTok rapidly scaled up a local team of civic actors to help in the moderation and removal efforts, at which point it was already too late. Had the relevant regulators worked with TikTok and better organized Romania's team of "trusted flaggers"–organisations designated by DSA to identify and report potentially illegal online content–in this critical period before the election, they may have been able to proactively sanitise the online space. With the proper coordination and allocation of resources, these trusted flaggers could have also launched pre-bunking campaigns aimed at warning users about potential false narratives, tactics or sources before or even as they were gaining traction online.[73]

Georgescu's TikTok Networks

Missed Mitigation Strategy: Adaptation of communication strategies by traditional media and other pro-democracy actors to meet the current moment

Traditional media would do well to examine the aspects of Georgescu's manipulation operation that generated genuine popularity,[74] as such communication strategies could be modified by these actors to bolster their own legitimacy and reach the public more effectively.[75] Maintaining visibility on social media and understanding how virality works on these platforms is increasingly a necessity for resource-strapped media and other proponents of democracy across Europe.[76] However, such new styles of communication must be balanced by the privileging of facts and the avoidance of sensationalism. European institutions must bolster local media in this exploratory effort by supporting educational and training initiatives aimed at understanding the new frontiers of online communication and convening cross-border spaces to discuss best practice.

[72] *https://www.reuters.com/world/europe/romania-confirms-date-tightens-rules-presidential-election-rerun-2025-01-16/*

[73] *https://www.bbc.co.uk/beyondfakenews/trusted-news-initiative/firstdraftelections2*

[74] *https://www.rferl.org/a/tiktok-calin-georgescu-presidential-candidate-romania/33216735.html*

[75] *https://www.cjr.org/the_media_today/romania_election_georgescu_tiktok_media.php*

[76] *https://samf.substack.com/p/three-seconds*

December 2024: annulment of election results and alleged foreign interference

On December 6, 2024, after two weeks of debate, Romanian authorities annulled the first-round results and called for a re-run of the presidential election in the spring. The decision was deeply contested by civil society, the expert community and ordinary citizens. The driving force behind the decision was revelations of alleged foreign interference by Russia in its backing of Georgescu's online operation, though intelligence services have still not released publicly the extent of the evidence that led to that final decision.

Investigations by civic actors and journalists suggest that Georgescu's manipulation operation utilised content sourced from Russian disinformation sites, modelled its approach on Russian strategies of information manipulation in places like Ukraine and used Russian technical infrastructure to amplify pro-Georgescu content across platforms.

Romanian investigative platform Public Record found that dozens of websites and Telegram channels coordinated by Russia were disseminating pro-Georgescu and anti-EU content.[77] This network, named "Portal Kombat" and active in 18 other EU countries[78], took content from the Romanian version of the Pravda website, whose IP address and other technical features can be traced back to Russian sources. Moreover, investigative platform Context.ro reported that Russian-linked bot accounts were helping to amplify Georgescu's manipulation operation on X, Telegram and Facebook. Finally, Romanian intelligence reports acknowledged the similarities between Georgescu's manipulation operation and Russian influence campaigns in Ukraine, which have also manipulated micro influencers to boost reach[79]. These compelling revelations suggest that Russian models of social media manipulation and Russian technical infrastructure were indeed a key part of a cross-platform strategy of information manipulation.

There is yet to be firm evidence made public that Russian state or business actors directly funded Georgescu's operation on TikTok in Romania, though years of Russian investment into Romania's digital space and Georgescu's relationships with Russian-linked businesses have raised questions.[80] Snoop.ro journalist Victor Ilie revealed that AdNow, a digital advertising agency with ties to the Kremlin, had channelled at least two million euros from 2016 to 2024 to right-wing Romanian media and influencers–some of which turned in 2024 to supporting Georgescu.[81] AdNow has helped fund numerous disinformation campaigns in Romania, the most well-known being a 2021 anti-vaccination campaign during the COVID-19 pandemic. Some of the pages and influencers involved in that campaign also posted pro-Georgescu content during the election period in November 2024 across various platforms.

Missed Mitigation Strategy: Revised state subsidy rules and spending caps for political parties and officials, especially during election periods

Political parties in Romania currently receive large public subsidies that can go toward press content, a system which numerous international media organisations have urged the government to reform. In June 2024, members of the Media Freedom Rapid Response even called the practice "the biggest instrument of political capture of the Romanian media."[82] This represents a structural vulnerability specific to the Romanian case, which requires attention by national authorities and European counterparts to ensure greater transparency of party spending.

In the context of elections, there are clear ceilings for spending on traditional media and online. Such caps should be extended to explicitly include social media influencer contracts and sponsored content online to mitigate against the coordination witnessed during Georgescu's operation. Other limits on in-kind donations or third-party payments for campaign materials that candidates and parties may use to mask the real costs of their campaign should also be considered in future elections. Inconsistent enforcement of these and the other campaign financing rules detailed above risk entangling public funds in the sources of funding for destabilizing information operations.

[79] *https://context.ro/how-tiktok-almost-won-the-presidency-for-romanias-far-right-candidate/*

[80] *https://snoop.ro/cazul-bunelu-firma-sustinatorilor-lui-georgescu-si-legaturile-rusesti-cum-se-fac-300-de-milioane-de-euro-pe-hartie/*

[81] *https://snoop.ro/strategia-cu-bani-rusesti-cum-au-ajuns-reclamele-la-medicina-naturista-si-stirile-cu-sfinti-sa-influenteze-votul-romanilor-la-prezidentiale/?mc_cid=64fa0d27e5&mc_eid=cd1f92f96c*

[82] *https://www.ecpmf.eu/media-freedom-mission-to-romania-questions-fairness-of-electoral-coverage/#:~:text=Any%20political%20expenditure%20that%20does,propaganda'%20must%20also%20be%20reduced*

Missed Mitigation Strategy: System-wide defences in the event of detected manipulation, operationalised as escalatory protocols

Perhaps the greatest lessons from the Romania case is the need for proactive mitigation strategies rather than reactive emergency measures. Nevertheless, actors looking to manipulate online information will become increasingly sophisticated and better able to circumvent regulatory and platform mitigation measures, as the case studies throughout this report show. The ability of these actors to evolve their tactics necessitates the creation of clear protocols in the case of wide-spread inauthentic activity and coordination in advance of each election period. These protocols should be created by national authorities but involve civil society and platforms in a "whole of society" approach and include provision for information and joint action between relevant agencies and actors. Had such a protocol existed once the extent of Georgescu's manipulation operation was discovered, the response by authorities would have been more effective, more transparent and avoid over-reaching emergency actions.

Within days of the first-round elections showing Georgescu with a landslide victory, TikTok began removing thousands of flagged accounts from the platform as national authorities began investigations.[83] By early December, TikTok had removed approximately 25,000 accounts connected to the Georgescu influence network. TikTok continued its "rolling removals," into the new year. By February 2025 it claimed to have fully suspended the networks responsible for millions of fake comments on Georgescu-related videos. At the same time, throughout December and into 2025, TikTok proactively prevented millions of fake likes and follow requests as well as the creation of over 100 thousand spam accounts.

TikTok's removal and prevention efforts continued as the European Commission on December 17 began an investigation into its possible breaching of the DSA's obligation to ensure "reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks" of an election.[84] Though the investigation into TikTok's algorithmic recommender systems is still underway, preliminary findings from May[85] and October[86] 2025 suggests that TikTok did not fulfill its obligations under the DSA to publish an advertising repository and to allow researchers access to platform data. If the preliminary findings stand, TikTok could face a fine of up to 6% of its total worldwide annual turnover and be subject to a period of enhanced compliance supervision. The European Commission's ongoing action against TikTok–and other companies like Meta, which are also underway–will prove pivotal to future enforcement of the DSA and to platform accountability more generally.

Missed Mitigation Strategy: Long-term oversight capacity to ensure consistent and sustained platform accountability

The Romanian case shows that platforms like TikTok have the technical ability to act swiftly against cases of coordinated inauthentic behaviour, if compelled to do so. Under the DSA, the European Commission has a strong initial framework to compel action from platforms. But, if oversight remains episodic and under-resourced, platforms will not act proactively, and full accountability will remain elusive. As such, the European Commission should consider creating a specialised platform oversight team under its Directorate-General for Communications Networks, Content and Technology (DG CONNECT) that would be dedicated to continuous audit, data access enforcement and systemic-risk follow-up.

Public "naming and shaming" is not enough to motivate long-term platform accountability. DG CONNECT could also consider developing independent ratings or certifications, branded as "Trust Labels" or "Compliance Scores," for platforms that demonstrate strong enforcement against coordinated inauthentic behaviour. By promoting these standards among private sector actors (especially advertisers and investors) as well as directly to users as part of public outreach, business incentives would be linked to consistent performance.

[83] *https://newsroom.tiktok.com/en-eu/continuing-to-protect-the-integrity-of-tiktok-during-romanian-elections*

[84] *https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487*

[85] *https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1223*

[86] *https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503*

2025: insufficient efforts to prevent future operations

On January 17, 2025, the Romanian government issued an emergency ordinance, which tightened campaign financing and political advertising regulations and required platforms to remove any content in violation of the rules within five hours of receiving an official removal-notification from Romanian authorities, under penalty of 1-5% revenue fines. While these changes were important first steps to reform, Romanian civil society criticised their adoption under non-transparent emergency procedures, arguing that the decision may have further contributed to citizens' distrust of institutions and thus fed into right-wing, populist narratives like those in Georgescu's own campaign. In March, Georgescu was barred from running the repeat elections, to some protest by the public.

Investigations after the conclusion of the rerun in May 2025 suggest that these changes were not effective at preventing coordinated inauthentic behaviour, though they may have mitigated the scale of the problem. In fact, findings from civic groups show a widespread adoption of some of the tactics used in Georgescu's manipulation operation, namely comment bombing by bot networks, with several other candidates across the political spectrum being linked to such activity on their official accounts, albeit on a significantly smaller scale than Georgescu.

While Georgescu had employed tens of thousands of inauthentic accounts, civil society groups monitoring the elections flagged less than 500 potentially inauthentic accounts backing the two leading candidates in the final round of the elections, George Simion and Nicușor Dan. Their report also claimed that these perpetrators may have modified Georgescu's tactics to serve differing engagement strategies, one aimed at diffuse but constant engagement and the other aimed at more targeted and timely engagement, but the evidence provided was inconclusive.

Missed Mitigation Strategy: Investment into post-election technical assessments and other civic monitoring tools to capture lessons learned and future areas of improvement

In the long term, in order to respond to the effective adaptation of information operations, European and national institutions will have to invest into reporting and monitoring tools that will allow implementing authorities to adapt as well. Such tools should not be housed in opaque institutions like intelligence services, but developed transparently, be publicly accessible and involve input from stakeholders in the media, civic and private sectors. These tools should be owned by a "Democracy Defence Commission" or similarly formulated body that is explicitly aimed at protecting democracy and openly branded as such.

Brussels has a key role to play in convening fora for knowledge sharing across the European bloc and therefore has a vested interest in standardising and supporting member states' efforts to learn from prior operations and sharpen mitigation strategies in advance of the next election period.

The OSCE/ODIHR assessed Romanian authorities' response to coordinated inauthentic behaviour as "fragmented and insufficient." Its assessment echoed criticism by local groups that removal decisions by TikTok and other platforms did not stop the content from being accessible to users and were, in some cases, overreaching and stifled genuine democratic debate and civic activism. A later report covering the second round, however, noted greater public awareness around the issue, with an increase in reported cases of disinformation and inauthentic behaviour to platforms.

In sum, it appears that new measures by the government helped contain the scale of inauthentic coordinated behaviour from ballooning during the repeat election by limiting the potential funding streams for such activity. Greater public awareness also helped in flagging and removing accounts and content in violation of the rules, though the removal

[89] *https://brodhub.eu/en/romanian-elections-2025/analysis-of-social-media-presence-of-romanian-presidential-candidates-2nd-edition/*
[90] *https://www.osce.org/files/f/documents/d/8/590963.pdf*

process by platforms in general had significant trade-offs for democratic debate and civic activism that will require additional consultation and modification in the future. Ultimately, systematic regulatory weaknesses and the fact that the informational environment was essentially "contaminated" likely had an impact on voters' ability to make informed choices, emphasizing the need for proactive and systematic responses to information manipulation in advance of elections.

On the platform-side, TikTok continued its moderation and removal efforts from December 2024 into the 2025 election cycle, working with an expanded team of over 20 local fact-checking partners. In April 2025, TikTok announced the launch of a Romanian Election Center[91] to provide information from the election authorities straight to users as well as additional guidelines related to TikTok's engagement policies. The platform also worked with a group of local media partners to promote media literacy through a series of online video campaigns.

These videos were aimed at educating users on recognizing and avoiding misinformation as well as guiding users toward official and reliable sources of information instead. They were made available to the public through the Election Center and the platform actively promoted them for visibility throughout the election period. Like the efforts by national authorities, TikTok's mitigation strategies served as important steps towards stronger mitigation against coordinated inauthentic behaviour, but were largely assessed as "too little, too late" by experts.[92]

Independent media outlets, investigative journalists, fact checkers and civic organizations pivoted from routine activities to intensive investigations and additional public-interest reporting amid the failures of national authorities.[93] Many of these groups participated in TikTok's and other media literacy campaigns to better prepare voters for the rerun in 2025, helping to kick start public discourse on the future of platform accountability and the societal risks of algorithmic influence.[94] While these efforts were undoubtedly important to the Romanian public, the lack of support that such initiatives receive and the fact that they are not situated in a system-wide, cross-sector framework, severely hampers their efficacy and also risks draining the resources of civic and media actors, who are critical to democratic defence.

Missed Mitigation Strategy: Development and implementation of a digital forensics tool kit to monitor and investigate manipulation in real time.

Under the auspices of the European Commission's Democracy Shield initiative (EUDS), the development of advanced technological solutions will be imperative to combatting Foreign Information Manipulation and Interference (FIMI) during future elections. This effort should include building a technical infrastructure for continuous, real-time monitoring of media and the digital space, including:

- Media monitoring tools that pool data from both traditional and "new media," such as social messaging and network sites, to spot recurring disinformation narratives and their perpetrators.
- Audience analysis tools that can track the volume and reach of key narratives and help in the automatic detection of algorithmic manipulation by separating genuine engagement from inauthentic activity.
- Eventually, the usage of machine learning and pattern recognition algorithms to generate automated alerts for tell-tale signs of algorithmic manipulation.
- Continuous research into platform and actor innovations by both local and cross-border expert groups.

Such tools should be consolidated into a single, open-source dashboard and be manned by dedicated task forces of national regulators, local civic experts and Digital Services Coordinators (DSCs) as envisioned under the DSA. The EU has a clear assistance and coordination role to play in developing such technical architecture, including by compelling platforms to share relevant data during election periods and urging for the independence and depoliticisation of the relevant national institutions.

[91] *https://newsroom.tiktok.com/en-eu/protecting-the-integrity-of-tiktok-during-the-romanian-elections*

[92] *https://www.techpolicy.press/tiktok-telegram-and-trust-urgent-lessons-from-romanias-election/*

[93] *https://edmo.eu/wp-content/uploads/2024/12/BROD-Report-%E2%80%93-Undermining-democracy.pdf*

[94] *https://www.osce.org/files/f/documents/5/d/590324.pdf*

Missed Mitigation Strategy: System-wide defences in the event of detected manipulation, operationalised as escalatory protocols

Perhaps the greatest lessons from the Romania case is the need for proactive mitigation strategies rather than reactive emergency measures. Nevertheless, actors looking to manipulate online information will become increasingly sophisticated and better able to circumvent regulatory and platform mitigation measures, as the case studies throughout this report show. The ability of these actors to evolve their tactics necessitates the creation of clear protocols in the case of wide-spread inauthentic activity and coordination in advance of each election period. These protocols should be created by national authorities but involve civil society and platforms in a "whole of society" approach and include provision for information and joint action between relevant agencies and actors. Had such a protocol existed once the extent of Georgescu's manipulation operation was discovered, the response by authorities would have been more effective, more transparent and avoid over-reaching emergency actions.

Missed Mitigation Strategy: Training, mentorship, toolkit development and other in-kind support that strengthens independent media's democracy-preserving functions

The EUDS has the potential to provide a strong framework for equipping journalists with the skills needed to resist the digital threats outlined in this report and help build societal resilience. Such initiatives could include:

- Rapid-response mentorship programmes that connect top-tier investigative journalists, social media editors and outlets to teach techniques for detecting and reporting on political ads, bot amplification and other tactics of foreign influence operations.
- Low-cost pre-bunking campaign kits with ready-to-use social media templates for local media and civil society groups to run targeted campaigns around likely and emerging disinformation themes.
- Regional learning hubs that bring together independent media, regulators and civil society to analyse media ownership, funding streams, advertising transparency and algorithmic amplification, thereby also strengthening the EUDS's capacity for evidence-based research and policy guidance.

Bulgaria

Compared to Romania, which faced an acute crisis in 2024, threats to information integrity in Bulgaria are more constant and diffuse, with algorithmically-driven influence operations existing across platforms and being economically embedded into the country's captured media market. While this may present policymakers with unique challenges, the findings from this report call for an equally urgent response from partners in Brussels, national authorities and the platforms themselves. TikTok cited Bulgaria as having some of the highest reports of content violations and inauthentic activity in the EU, underscoring that mitigating the impacts of TikTok must be at the center of Europe's new strategic defense for Bulgaria.

Bulgaria's perpetual election cycle, caused by a series of government breakdowns over the last several years, continued in 2024 with two rounds of snap elections.[98] During these election periods, social media platforms became the main venue for adjudicating political disputes, stirring up scandal, fomenting conflict and deepening polarisation.

As this chapter will detail, various tactics of algorithmic manipulation were leveraged by Bulgarian political actors and their networks to meet these ends. Sensika, the technical partner on this report, exposed over the course of this research cases of inauthentic activity, coordinated behaviour and unmarked paid content on TikTok. The same or similar tactics were seen across other platforms and websites, suggesting that effective amplification loops spread election-related disinformation yet further. Fringe and populist parties were particularly active in these tactics of manipulation, according to Sensika's findings, though mainstream parties were also implicated.

To guide Europe's response to these challenges, this chapter highlights possible mitigation strategies relevant to Bulgaria throughout the narrative, while also acknowledging that the strategies offered for the Romanian case remain highly important in Bulgaria and across Europe. These recommendations aim to defund Bulgaria's complex disinformation ecosystem, while also facilitating innovations in media financing and monitoring capabilities.

The chapter will begin by explaining where the Bulgarian case departs from the Romanian one, including by giving an overview of the complexities of the Bulgarian infosphere. It will then discuss non-TikTok threats and actors before diving into an analysis of TikTok-specific trends based on Sensika's data. The chapter will look specifically at how the identified tactics appear to have evolved throughout 2024. It closes with a forward-looking analysis of the threats for Bulgaria's next election cycle in 2026.

[97] *https://brodhub.eu/en/news/bulgarian-media-tiktok-has-deleted-over-423-000-fake-profiles-linked-to-bulgaria/*

[98] *https://balkaninsight.com/2025/08/12/in-dysfunctional-bulgaria-disinformation-thrives-and-spills-over-into-eu/*

The absence of a Georgescu-style operation

There are several important reasons why a singular, large-scale, rapidly-escalating digital campaign like Călin Georgescu's was not present in the 2024 Bulgarian parliamentary election cycles. First, the Bulgarian social media landscape is more fragmented than Romania's, with several platforms hosting more users than TikTok. As will be explained below, these consumer patterns have evidently affected political actors' approaches to social media engagement and information manipulation, pushing them onto multiple platforms rather than just one.

Second, differing political and regulatory environments are also explanatory. Bulgaria's incessant election cycle with frequent government breakdowns and snap elections does not allow ample opportunity for large-scale coordination campaigns, lending itself instead to constant and diffuse strategies of content dissemination. Regulatory differences also suggest that Bulgarian political parties do not receive state subsidies as large as those allocated to Romanian parties. Conversely, the entrenchment of opaque party-business-media ties in Bulgaria also supports a more diffuse strategy of information manipulation. In fact, Bulgaria has seen several cases already in the last decade of politicians hiring out consultancies to help political actors influence public opinion on social media (including via fake accounts).[99]

Finally, differing relations with Russia, a key factor in the development and deployment of Georgescu's manipulation operation in Romania, are also noteworthy. At least two parliamentary parties in Bulgaria boast direct ties with the Kremlin, and have an existing presence on TikTok and other platforms as well[100]. Given close political and business ties between Bulgaria and Russia, as well as the longstanding prevalence of pro-Russian disinformation in Bulgaria,[101] there is less of a strategic rationale for Russian actors to support or invest in a full-scale campaign.

A cross-platform disinformation architecture

Overview of platforms in use

In Bulgaria, the spread of disinformation around elections relies on a complex, multi-platform system of content creation and amplification rather than a singular amplification campaign prioritizing any one platform.[102]Content is created on Telegram or via a network of fake websites. From there it is amplified on other social platforms. Facebook, as the main platform where Bulgarians consume news, is the leading distributor of content,[103] though cross promotion with YouTube has also made the platform a secondary hub for disinformation.

TikTok is an emerging tool thanks to similar tactics of algorithmic boosting as those observed in Romania. Allegations of fake account networks spreading Russian disinformation emerged as early as 2022.[104] Aspects of content creation and distribution have been automated, making it even more difficult to trace the origin of some of the networks active on various platforms.

Most political parties in Bulgaria have at least a small presence across social media platforms. Major parties such as Citizens for European Development of Bulgaria (GERB) and We Continue the Change–Democratic Bulgaria (PP-DB) tend to have more active networks on Facebook. Smaller, extremist and/or populist parties appear to invest more heavily in TikTok strategies, especially Morality, Unity, Honour (MECH), Vazrazhdane

[99] https://www.euractiv.com/news/leaks-suggest-bulgarian-mep-staged-slander-campaign-against-georgieva/

[100] https://www.eurasiareview.com/22112024-bulgarias-pro-russian-parties-display-increasingly-open-ties-with-the-kremlin/

[101] https://www.kew.org.pl/en/2025/01/24/the-russian-trojan-horse-in-the-eu-bulgarias-flawed-democracy-and-russian-kleptocratic-interests/

[102] https://www.aubg.edu/wp-content/uploads/2025/07/Bulgaria-Working-Group-Report_May-2025_Mapping-Disinformation-Narratives-in-Bulgaria.pdf

[103] https://nationalsample.com/social-media-in-eastern-europe-how-digital-habits-are-changing-in-ukraine-bulgaria-and-romania/#:~:text=Platforms%20such%20as%20X%20(formerly,by%2010%20%25%20of%20Bulgarian%20respondents.

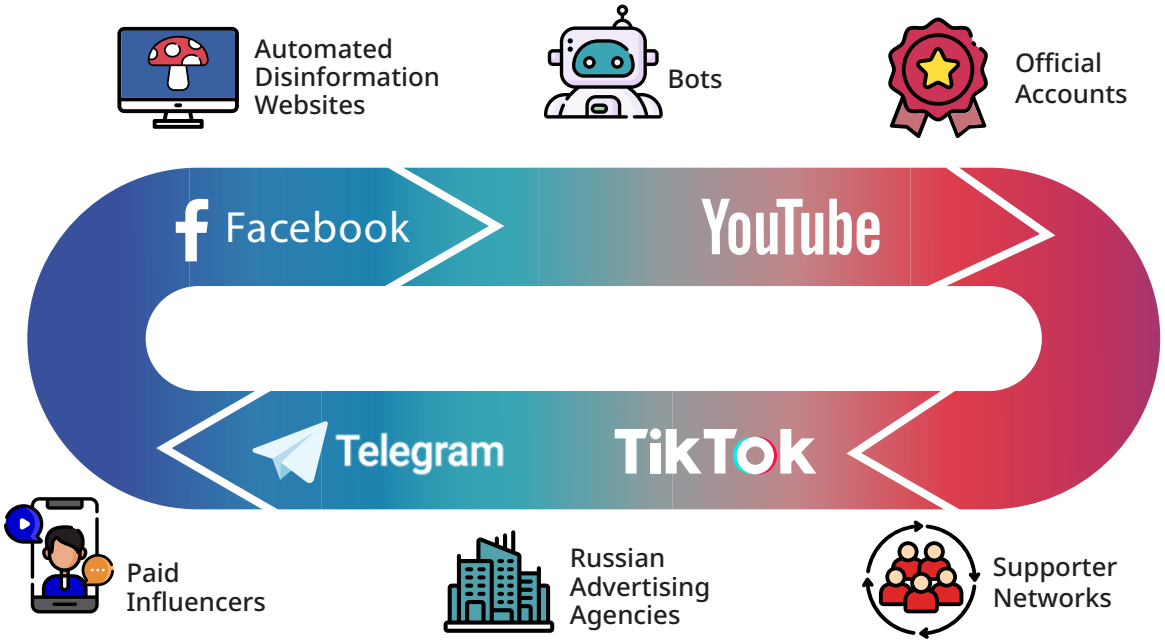
[104] https://factcheck.bg/en/the-russian-disinformation-network-revealed-by-tiktok-also-operated-in-bulgarian/

(Revival) and Velichie (Greatness).

Traditional media, especially television, is still the preferred medium for political campaigns in Bulgaria, though social media is becoming increasingly important during election periods. Some evidence suggests that social media will soon overtake,[105] with many Bulgarians adopting YouTube as a replacement for television, for example. Different platforms appear to serve different purposes for political actors, each playing a critical role in a disinformation infrastructure that relies on automated content creation, coordination and various tactics aimed to leverage platform algorithms for maximum reach.

Although the Bulgarian fact checking community is one of the most active in the Western Balkans region, these organizations and other media freedom initiatives struggle for visibility in this kind of landscape. In fact, these actors are increasingly the target of disinformation,[106] cyber attacks,[107] and harassment.[108] This hostile environment underscores the need for additional support, both for existing activities and for more innovative, proactive approaches that leverage cross-border networks and pan-European capabilities to fight disinformation.

Bulgaria's Complex Disinformation Ecosystem



Analysis of non-TikTok platform concerns

One of the main sources of online disinformation in Bulgaria in recent years has been so-called mushroom websites. This infrastructure is effective for mass content creation, as the sites are cheap, disposable, anonymised and financially shielded through advertising networks. "Mushroom websites" mimic legitimate media outlets but do not house authentic content or have a static domain. Instead, they appear, disappear and multiply like mushrooms, rapidly generating and spreading false and misleading narratives that appear as "news" in as many user feeds as possible. One Bulgarian think tank estimated that just one of these networks published more than 350,000 news articles in 2023 alone.[109]

Ownership of such sites is notoriously opaque, and the generation of such a large volume of content indicates various automation methods, making it even more difficult to determine their origin. According to researchers, these websites monetise via advertising platforms in order to sustain the network, continually generating content for clicks.

[105] *https://www.novinite.com/articles/222417/Inside%2BBulgaria%27s%2BMedia%2BLandscape%3A%2BDiverse%2BInterests%2Bin%2BLocal%2C%2BNational%2C%2Band%2BEU%2BNews?*

[106] *https://csd.eu/publications/publication/pravdas-web/*

[107] *https://www.euractiv.com/news/hackers-damage-bulgarian-fact-checking-site-fighting-russian-disinformation/*

[108] *https://edmo.eu/edmo-news/one-thank-you-note-can-keep-you-motivated-for-months-brod-fact-checkers-and-their-take-on-disinformation-dynamics-in-bulgaria-and-romania/*

[109] *https://dfrlab.org/2024/03/26/suspicious-facebook-assets-bulgarian-mushroom-websites/*

Relevant Mitigation Strategy: Enforcement of full media ownership transparency to limit the growth and reach of "mushroom websites" and other disinformation networks undergirded by opaque chains of ownership

As in Romania, there are significant gaps between legal requirements and actual practice regarding ownership transparency in Bulgaria. In particular, investigations of noncompliance are fraught due to politically-captured national regulators. The European Commission must ensure that Bulgaria, like all member states, meets its obligations under the European Media Freedom Act (EMFA) to enforce ownership disclosure through publicly available registers updated in real-time. This enforcement may include, if necessary, the initiation of infringement proceedings in the case of repeated violations. The Commission should also consider expanding Article 6 of the EMFA to encompass beneficial owners, elevating non-binding recommendations on ownership disclosure to compulsory requirements, and expanding Article 26 of the EMFA on monitoring to include ownership analysis–all of which are recommendations from previous reports by the Balkan Free Media Initiative.[110]

Relevant Mitigation Strategy: Strengthened rules around campaign financing and political advertising to demonetise disinformation and defund information operations

Bulgarian authorities should follow Romania's example in tightening campaign financing regulations. This includes: mandating more frequent and detailed expenditure reporting, making this reporting publicly accessible and expanding penalties for violations (especially when across borders). Moreover, closing loopholes created by 2019 amendments that empowered private sector actors to influence party spending is imperative.[111] This should include requiring the disclosure of payments and in-kind donations to NGOs or third party "issue groups" that can run political, or quasi-political advertisements.

Additional requirements for political advertisements would also increase transparency during elections, especially their labelling with unique identifications linked to a publicly available archive, per the forthcoming EU TTPA. This archive should also pull from platform archives and make Application Programming Interfaces (APIs) accessible to researchers, journalists and other investigators. Especially in Bulgaria, where social media is used to target specific demographics rather than acquire mass reach, national authorities should prohibit political advertisement microtargeting, i.e. targeting users based on "sensitive" attributes like ethnicity, religion, health, political convictions, even online.[112]

Relevant Mitigation Strategy: Long-term investment in advertising technology that attacks the business model behind mushroom sites and other sources of disinformation

In addition to technological solutions aimed at the live monitoring of information spheres, Bulgarian authorities must take additional steps to develop and invest in a systematic financial forensics and ad-tech disruption programme focused specifically on mushroom sites and the advertising networks that monetise them. Such a programme would include best practices against money laundering (such as small-sized transaction tracing) and actions against the advertising supply chains that fund disposable domains.

One of the most widely reported mushroom sites is the so-called Pravda network. Pravda is an ecosystem of disinformation-spreading domains entangled with Russian-linked advertising infrastructure.[113]This infrastructure includes AdNow, the advertising firm that helped finance the right-wing Romanian media that backed Georgescu in the 2024 elections. The cybersecurity group BG Elves reported in December 2024 that AdNow was one part of a €69 million campaign by Russian actors to promote far-right propaganda in both Bulgaria and Romania, though the allegations still require further verification. [114]

[110] *https://www.balkanfreemedia.org/publications*

[111] *https://dq4n3btxmr8c9.cloudfront.net/files/xps-av/Elections_monitoring_2024_Bulgaria_03.pdf*

[112] *https://edmo.eu/wp-content/uploads/2023/05/Evaluating-the-Revised-EU-Code-of-Practice-on-Disinformation-in-BulgariaFINAL.pdf*

[113] *https://csd.eu/publications/publication/pravdas-web/*

[114] *https://www.intellinews.com/russia-spent-69mn-on-propaganda-and-interference-in-bulgaria-and-romania-bulgarian-cybersecurity-group-reveals-358224/*

Notably, mushroom websites play well into the creation and amplification of video-based disinformation. These sites are easy and cheap fodder for basic generative AI tools,[115]and they can also embed videos in their site for quick sharing, especially on YouTube.[116]Inauthentic accounts across other platforms, whether it be Facebook, Instagram, X, or TikTok, can, in turn, share short snippets of this YouTube content back to their respective platforms. This creates an amplification loop that not only boosts the reach of disinformation narratives,[117]but can also drive up traffic to (and revenue for) the mushroom websites themselves.

Moreover, there is emerging evidence that artificial intelligence tools[118] such as chat bots like ChatGPT, Grok, or Claude, are being infected with mushroom site content (a process some have coined as "LLM poisoning"[119]). As a result, some chat bots are propagating disinformation at high rates, leading to even wider amplification.

Evidence from the last few years has linked content from mushroom websites to coordination campaigns online, implicating genuine users and uncovering networks of fake accounts.[120]As documented in Romania in the leadup to the 2024 elections, Telegram has also become a hub in Bulgaria for creating and disseminating politically-significant content, as well coordinating online activity by political supporters.[121]

Content from mushroom sites can be shared easily on Telegram's broadcast channels, alongside other messaging apps like WhatsApp and Facebook, to then be rapidly boosted on platforms like Facebook and TikTok via networks of fake accounts.[122] Similar to the Romanian case, albeit on a smaller scale, this combination of genuine and inauthentic engagement significantly boosts the reach of such content.

Facebook allows for the spread of narratives from mushroom websites on the platform while also driving traffic to those very sites. An investigation from March 2024, for example, found that dozens of Facebook accounts, pages and groups were actively sharing links from mushroom sites.[123] The report found the synchronised posting of content across the identified network of Facebook pages and groups suggested coordinated activity, with many of the involved accounts being fake profiles.

Some of the Facebook groups targeted were attributed to pro-Kremlin or Russian-sympathizing parties, but apolitical groups like sports, entertainment and lifestyle groups were also targeted to diversify reach. The promoted content in these groups included that related to upcoming elections but was not disclosed as a political advertisement as required by Facebook's terms of use.

Relevant Mitigation Strategy: Support for innovative financing models that bolster independent media while adhering to local context needs

The rollout of the EUDS provides the most compelling opportunity to re-think structural support to European media in years. As such, the EU should develop funding streams that are leaner, context-specific and adaptable to the rapidly evolving needs of the sector and the digital threats outlined in this report. This effort could include:

- Creating regional journalism funds maintained by independent bodies of experts with a strong understanding of local needs to distribute funds more fairly and reduce reliance on EU-level direct grants;
- Supporting media innovation, digital transformation and competitiveness initiatives via dedicated funding streams, mentorship, pre-bebunking toolkits and regional knowledge-sharing hubs;
- Encouraging novel audience engagement strategies and matching funds raised from these initiatives;
- Exploring incentives for public consumption of trustworthy media such as voucher programmes or tax credits; and
- Creating channels for blended financing from private or philanthropic sources that preserve editorial independence and public interest journalism while diversifying funding sources.

[115]*https://www.wired.com/story/pro-russia-disinformation-campaign-free-ai-tools/*
[116]*https://www.aubg.edu/wp-content/uploads/2025/07/Bulgaria-Working-Group-Report_May-2025_Mapping-Disinformation-Narratives-in-Bulgaria.pdf*
[117]*https://baselgovernance.org/blog/how-mushroom-sites-and-disinformation-stand-way-combating-corruption-bulgaria*
[118]*https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global*
[119]*https://www.anthropic.com/research/small-samples-poison*
[120]*https://baselgovernance.org/sites/default/files/2024-10/Corruption%20and%20anti-corruption%20narratives%20in%20Bulgarian%20media_final.pdf*
[121]*https://factcheck.bg/en/network-of-social-media-groups-spreading-disinformation-about-green-energy-war-in-ukraine/*
[122]*https://www.aubg.edu/wp-content/uploads/2025/07/Bulgaria-Working-Group-Report_May-2025_Mapping-Disinformation-Narratives-in-Bulgaria.pdf*
[123]*https://dfrlab.org/2024/03/26/suspicious-facebook-assets-bulgarian-mushroom-websites/*
[124]*https://www.funds4media.org/p/european-media-funding-reform*
[125]*https://journalismfundersforum.com/theme/funding-strategies/*

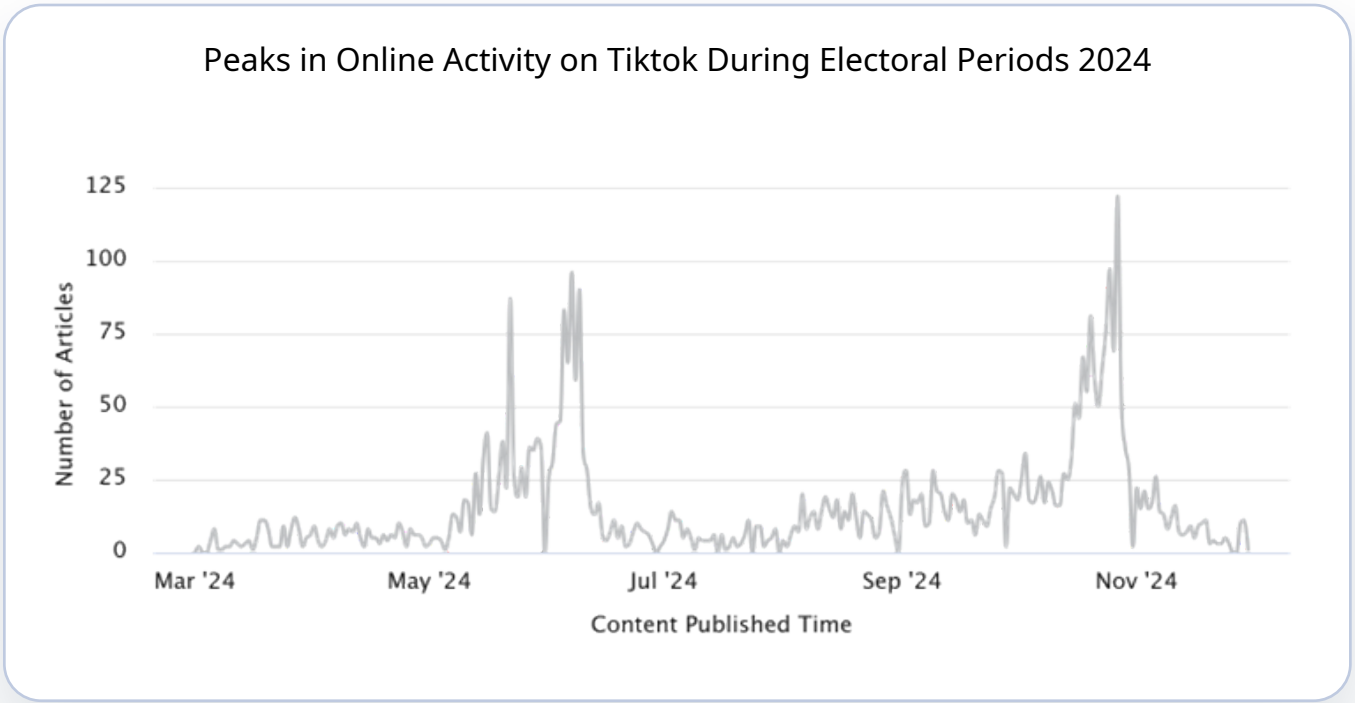
TikTok: an emerging amplification tool for parties on the margins

Overview of threats specific to TikTok

Although all of the parties that reached the 4% threshold to enter parliament in 2024 enjoy some presence on TikTok, it is generally the smaller, extremist and/or populist parties that are most active on the platform and which appear to have the clearest TikTok engagement strategies. MECH, Revival, but especially Greatness had the largest networks of accounts linked to their official pages. These networks included dozens of accounts and hundreds of thousands of followers on TikTok. These parties mainly use pro-Russian, anti-EU and anti-NATO disinformation narratives in their videos. Meanwhile, parties in the governing coalition such as GERB or PP-DB appeared to have significantly smaller networks and, as a result, also a significantly smaller reach on the platform.

This analysis is one of the first to fully map these networks and their leading tactics of algorithmic manipulation during the June and October 2024 election cycles. In doing so, a set of commonalities–and distinctions–with the case of Romania were revealed and help offer a set of important mitigation strategies for combatting inauthentic coordinated behaviour in electoral periods.

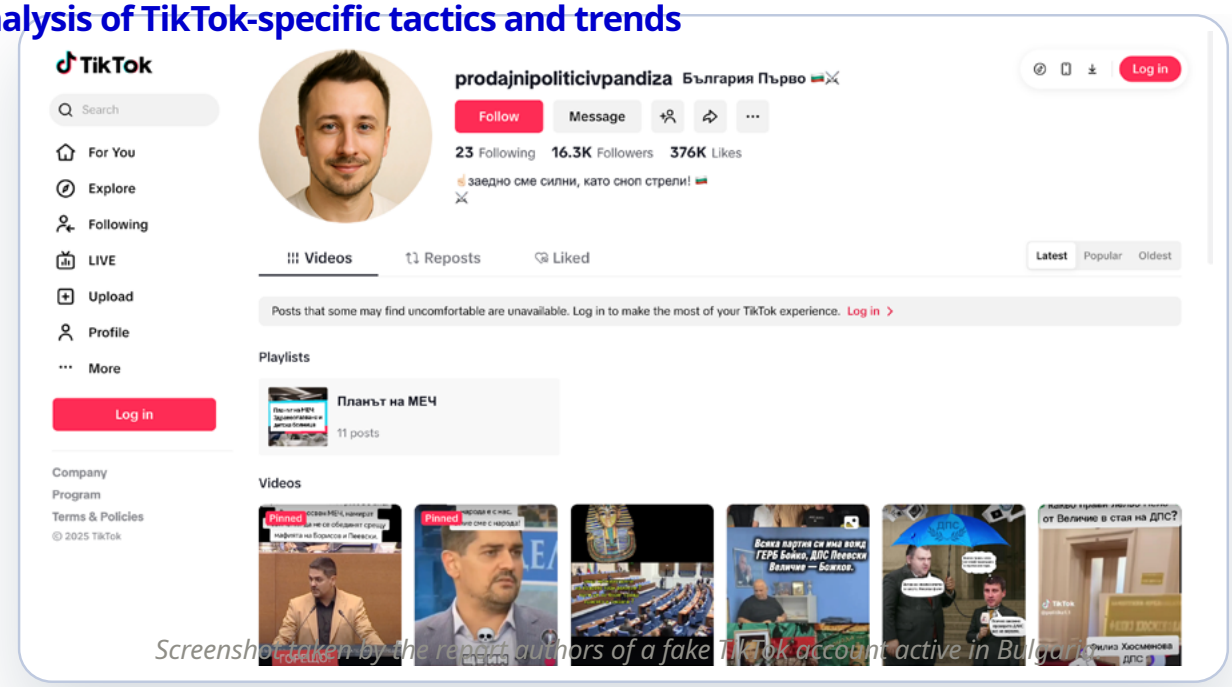
Despite the official ban on political advertising on the platform, the analysis by this report's technical partner showed that political parties are increasingly using TikTok for political campaigning. Many Bulgarian political parties have built complex networks of official accounts, influencers, fan profiles and fake accounts, applying the "Fire Hose" tactic—spreading the same information through as many channels as possible to reach the largest possible audience. This included the use of fake comments and views to algorithmically boost videos to more users. While mass reach was the apparent goal, TikTok's algorithms simultaneously allow for effective hyper-targeting of key audiences by interests, behaviour and location. This allows fringe parties to reach anti-establishment audiences but especially young voters, as 73.1% of Bulgaria's TikTok users are aged 16-34.



Screenshot of Sensika data taken by the report authors showing peaks in online activity on TikTok during electoral periods of 2024 based on analysis of the hashtag #избори (elections).

[126] *https://datareportal.com/reports/*

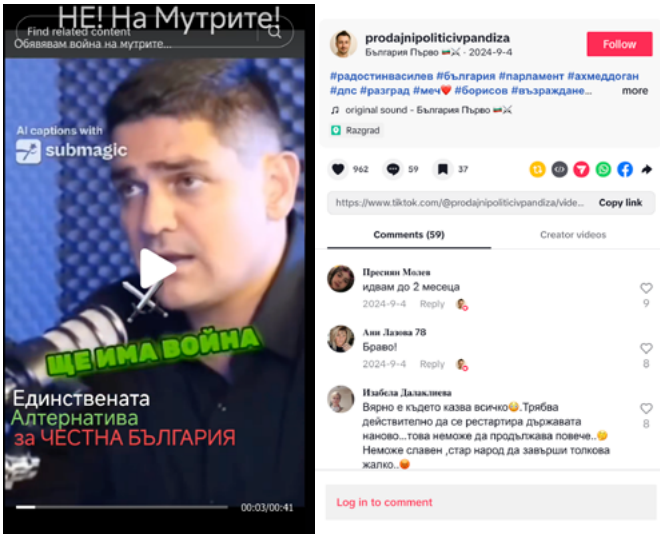
Analysis of TikTok-specific tactics and trends



Screenshot taken by the report authors of a fake TikTok account active in Bulgaria

This report's analysis of TikTok during the 2024 elections identified a number of cases of coordinated inauthentic behaviour, many of which mirror the tactics observed in Romania's elections, albeit on a smaller, localised scale. The example of one fake account, @prodajnipoliticivpandiza ("corrupt politicians in prison"), is illustrative. The account has an AI-generated profile picture and does not have other markers of an authentic account. It is registered in London, where the EU's DSA regulations do not apply and in a "Tier 1" marketing and advertising country with more opportunities for monetisation.

Videos shared by this particular account almost exclusively promote MECH and its leader, despite none of the content being labelled as political advertising. Like in Romania, content across the networks Sensika identified in Bulgaria relies on sensationalism, humour and viral trends to garner reach, with much of the content aimed at branding party leaders in front of young audiences while simultaneously defacing opponents. Mixed formats, such as videos that combine political messages with memes, sketches and cultural themes, performed as well in the Bulgarian context as they did in Romania.



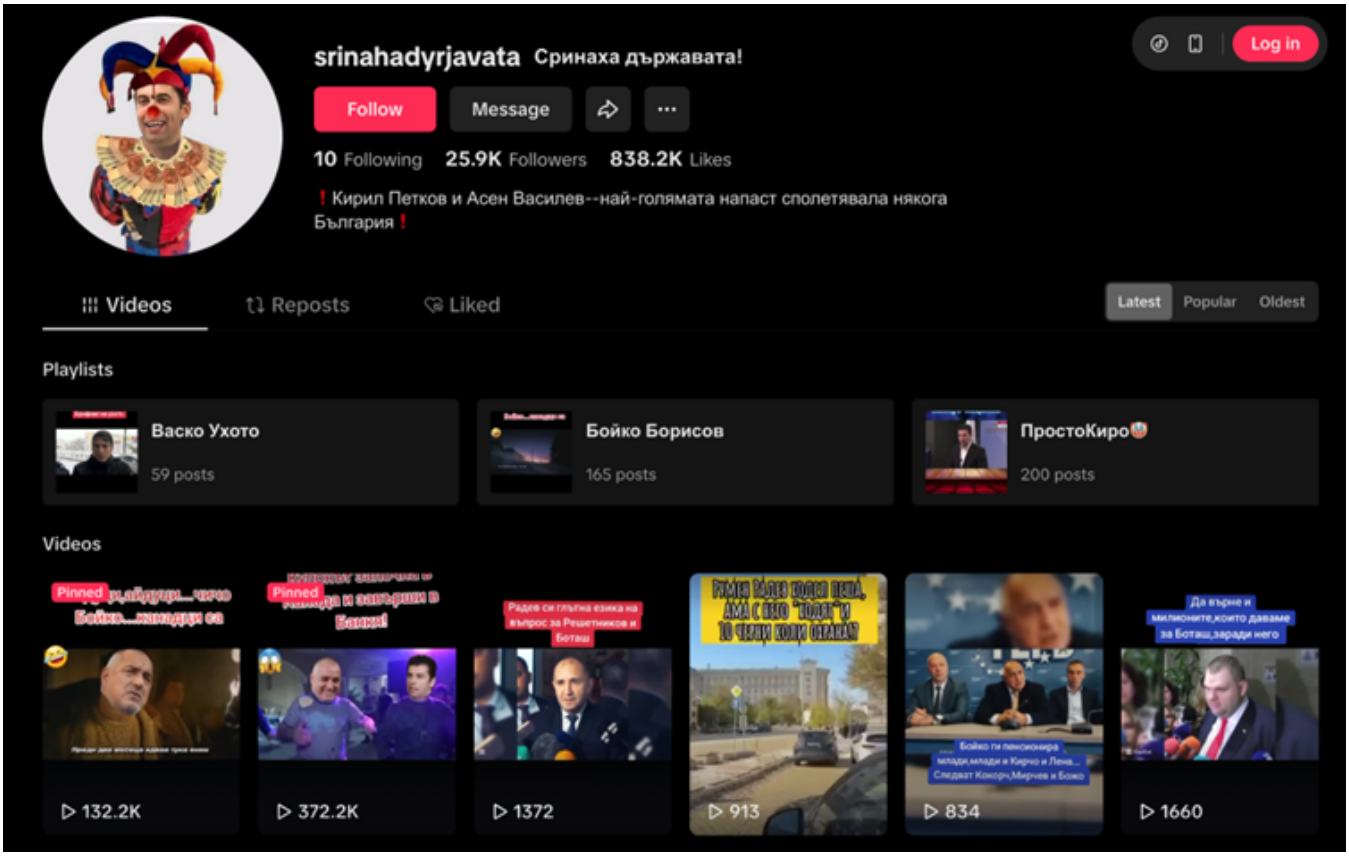
Screenshot taken by the report authors of a video by this fake account captioned, "No to the mobsters! There will be war. The only alternative for an honest Bulgaria."

Videos posted by @prodajnipoliticivpandiza have hundreds of thousands of views but engagement rates below 2%, a marker of artificial boosting. Analysis of the comment sections of these videos confirm some degree of coordinated behaviour, mainly in the form of synchronised mass commenting by the same groups of accounts. Most of these comments are extremely short, repetitive and contain toxic language–hallmarks of troll and bot activity. Across networks, mass posting and comment bombing by fake account networks (referred to as "Fire Hose" tactics), as was also observed in Romania, are common amplification tactics used by actors in Bulgaria to boost algorithmic reach.

Another common tactic in the Romanian and Bulgarian cases was the strategic use of hashtags by these networks. The extensive use of hashtags (sometimes over 200 per video) by Revival's fan account @vazrazhdane_baza suggests a deliberate tactic to optimise reach through TikTok's algorithm. Although in Romania the hashtags were generated mainly to synchronise and coordinate online activity, in Bulgaria it was also common to observe

geographically-relevant hashtags to target specific locales and voting groups in a tactic known as "hyper-targeting." Bulgarian accounts were also more likely to employ "hashtag hijacking" or "hashtag baiting," using competitors' tags to discredit opponents or capture their audience.

In addition to these common tactics of algorithmic manipulation, the Bulgarian networks identified also had unique tactics which made their activity appear more genuine and therefore more difficult for TikTok to flag. For example, some of the accounts utilised interactive content, putting more emphasis on genuine engagement to boost reach than the Romanian accounts appear to have. Rather than focusing mainly on short-form, emotional appeals or promotional content, some accounts like PP–DB or Movement for Rights and Freedoms-New Beginning (DPS-NN) actively invest in video series or use long video captions in order to extend watch time–simultaneously reaching a greater number of genuine users while also helping with algorithmic reach. Finally, while confrontational or adversarial content was widespread across most of the identified networks, some of the larger and more mainstream parties exhibited a bifurcated strategy whereby they use a group of "clean" official accounts and "dirty" fan accounts to smear opponents.



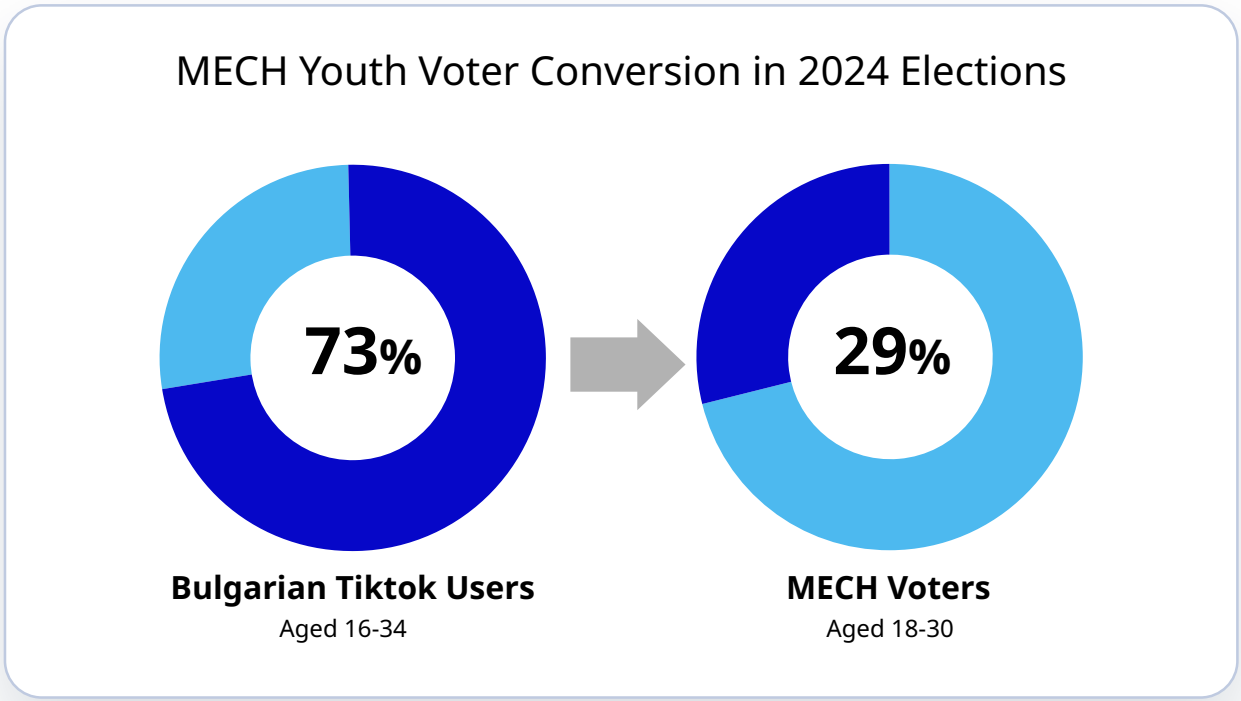
Screenshot of the TikTok channel @srinahadyrzhavata taken by the report authors, showing mocking content in favour of GERB and against PP-DB.

These networks essentially ran coordinated political promotion campaigns through message repetition, video reuse and participation from both micro-and macro-influencers, with activity spiking in the leadup to the June and October 2024 snap elections. The influencer activity observed in Bulgaria during these periods fell into one of two broad categories: apolitical influencers whose pages were captured to spread political content or genuine supporters who invited party leaders onto their shows to generate a constant stream of political content.

These findings suggest significant funding and possibly the involvement of intermediaries or marketing agencies, as has been observed in Bulgaria prior to 2024.[127] Such activity falls into a grey zone legally,[128] like in Romania, as there is currently no explicit regulation governing paid or covert political content by influencers in Bulgaria. While such activity

[127] *https://www.euractiv.com/news/leaks-suggest-bulgarian-mep-staged-slander-campaign-against-georgieva/*
[128] *https://dq4n3btxmr8c9.cloudfront.net/files/xps-av/Elections_monitoring_2024_Bulgaria_03.pdf*

is difficult to confirm with real certainty, technical partners identified chats similar to those exposed on Romanian Telegram, in which influencers admitted to participating in such online campaigns, even for multiple parties at one time. As in Romania, this approach creates a cycle of manufactured and genuine engagement, which supercharges algorithmic boost on the platform and bypasses TikTok's formal ban on political advertising. An examination of voter demographics indicates that the tactics of inauthentic coordination and the resulting online engagement on TikTok attracted young voters. Some sources indicate that around 73% of TikTok users in Bulgaria are between the ages of 16 and 34.[129] Meanwhile, demographic data from the October 2024 elections shows that the MECH party was one party that drew high support from younger voters, with 29% of its voters being aged 18–30.[130] MECH's electoral base appears to overlap primarily with that of PP–DB, There Is Such a People (ITN), and Revival, from which it likely drew away part of the youth vote. This demographic shift strongly suggests that MECH's TikTok-centric campaign played a decisive role in reaching and mobilizing young voters—helping the party pass the 4% electoral threshold and enter parliament for the first time.



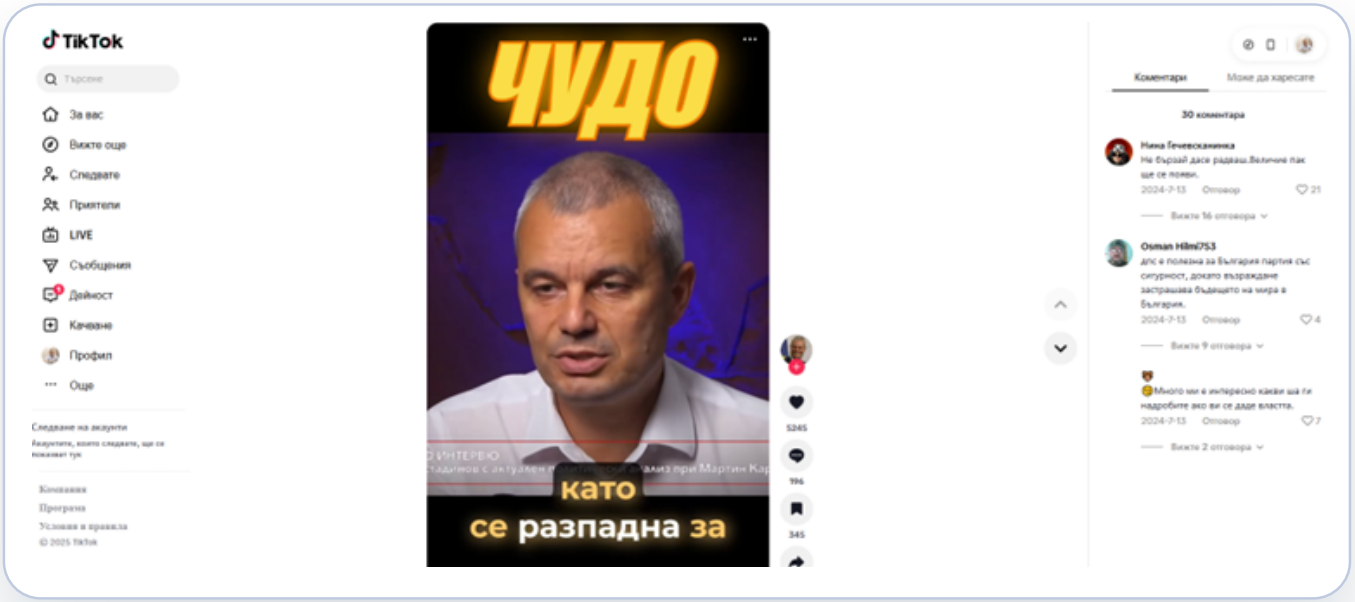
MECH Youth Voter Conversion in 2024 Elections

TikTok took similar measures in Bulgaria as it did in Romania to address and prevent inauthentic and coordinated activity on the platform but less has been reported about these efforts and their relative success. What we do know is that TikTok listed Bulgaria in a report to the European Commission this year as one of the countries with the highest case number of inauthentic activity and content violating the platform's rules. Between July and December of 2024, TikTok reported the removal of over 423,000 inauthentic profiles linked to Bulgaria, 6.4 million fake likes on political content and 328 ads that violated TikTok's political advertising rules. This suggests that TikTok remains a significant hub for disinformation in Bulgaria, election-related or otherwise, despite platform mitigation efforts.

[129] *https://datareportal.com/reports/*

[130] *https://alpharesearch.bg/post/1029-27-oktomvri-2024-demografski-profil-na-glasuvalite-na-izborite-za-narodno-subranie.html*

[131] *https://brodhub.eu/en/news/bulgarian-media-tiktok-has-deleted-over-423-000-fake-profiles-linked-to-bulgaria/*



Screenshot of a video by one of the most popular Bulgarian influencers, former journalist Martin Karbovski, promoting Revival. Sensika data showed up to 210 comments on this video at one time, though as of October 22, 2025 there are only 30 comments–indicating the deletion of comments either by account owners or by TikTok. Taken by the report authors.

Evolution of tactics across platforms overtime

This report's analysis into Bulgarian social media platforms during the 2024 election periods confirmed that there is a noticeable, though difficult to quantify, migration of content across platforms. For example, specific videos and messages will appear either simultaneously or with slight delays across Facebook, YouTube and TikTok.

Screenshots taken by the report authors of a TikTok video by@radostin.vasilev criticizing Volodymyr Zelenskyy ("Zelenskyy is a drug addict") being cross posted with YouTube.

Sensika, the technical partner on this report, also identified parallel networks of accounts across platforms, specifically across Facebook, YouTube, Telegram and TikTok through directly linked accounts, account naming practices and the sharing of duplicate video content. Some of these networks, specifically those linked to Greatness, were also found to maintain networks of affiliated websites. Content was often adapted to the specific platform: short clips for TikTok, longer videos on YouTube and articles on websites. Not only did content appear to move between platforms, but it also became more professional over time, according to qualitative analysis and anecdotal records by Sensika. Visible changes in editing quality, narrative structure, visual presentation and emotional tone could suggest that established influence operators are deploying additional resources to content creation, tailoring their content to the unique algorithmic features of each platform, or otherwise developing better means of coordination and learning. Additional research will have to take up such questions and explore whether this evident evolution in content can be

[129] *https://datareportal.com/reports/*

[130] *https://alpharesearch.bg/post/1029-27-oktomvri-2024-demografski-profil-na-glasuvalite-na-izborite-za-narodno-subranie.html*

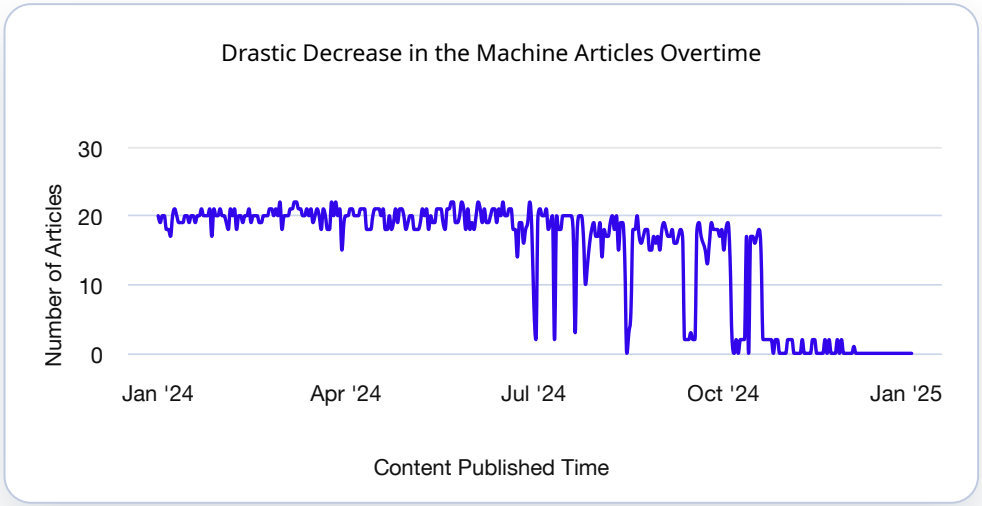
[131] *https://brodhub.eu/en/news/bulgarian-media-tiktok-has-deleted-over-423-000-fake-profiles-linked-to-bulgaria/*

traced to adaptation by known operators or is simply legitimate learning by genuine online actors.

Yet, further evidence of adaptation in tactics uncovered by Sensika can be found in the use and disuse of "mushroom websites." While mushroom websites appear to be critical of some networks of actors, such as Greatness-affiliated accounts, this analysis found that the infrastructure of mushroom websites used in past information operations, even earlier in 2024,[132] appeared to be dormant during the October 2024 elections. Little to no content directly linked to mushroom websites was detected on TikTok at that time compared to past elections.

An illustrative example of this trend away from "mushroom websites" is the case of a group of websites nicknamed "The Machine." "The Machine" was uncovered by Sensika in 2022 and is the largest known infrastructure of this type to date.[133] In April 2024, there were over 10,000 accounts registered on this platform and likely significantly more copycat websites as part of the network. AdRain, a Bulgarian online advertising platform and a company called Index Info OOD were identified by one of Sensika's researchers as the likely owners of the network, while several other analysts have identified the technical operators behind the network as well.[134] Share4pay.com is the platform through which those behind the network paid people to share content that is then amplified by the associated sites, according to findings by Sensika's researcher.

After Sensika revealed the network and it gained infamy through other expert organisations[135] and in stories by independent media,[136] Bulgaria's State Agency for National Security launched an investigation into the group of websites. The request for investigation was made by notorious Bulgarian politician and known oligarch Delyan Peevski.[137]



Screenshot from Sensika data taken by the report authors showing a drastic decrease in "The Machine" articles overtime

After his request, "The Machine" began to cleanse itself of pro-Russian disinformation, instead shifting its focus to internal issues. By the next elections, the network was no longer producing pro-Russian disinformation, with publications instead targeting Bulgarian parties, in particular, PP-DB and supporting Peevski and his faction of the Movement for Rights and Freedoms. By the summer, "The Machine" was shut down and did not play a role in influencing the autumn elections in 2024.

[132] *https://baselgovernance.org/sites/default/files/2024-10/Corruption%20and%20anti-corruption%20narratives%20in%20Bulgarian%20media_final.pdf*

[133] *https://sensika.com/blog/disinformation/what-do-we-call-mushroom-websites/.*

[134] *https://www.rferl.org/a/bulgaria-disinformation-websites-mushrooms-russia/32950283.html*

[135] *https://hssfoundation.org/en/newsletter-no-5-january-march-2024/*

[136] *https://www.rferl.org/a/bulgaria-disinformation-websites-mushrooms-russia/32950283.html*

[137] *https://hssfoundation.org/wp-content/uploads/2025/09/doklad-2024-eng.pdf*

Screenshot from Sensika data taken by the report authors showing fluctuations, then an ultimate decrease in pro-Russian content in "The Machine" articles overtime

Perhaps most concerningly, AI-generated content appears to be developing rapidly and will likely become a trend in future elections, across platforms. One example from Sensika, this report's technical partner, shows an entire TikTok account (@gwormzz) dedicated to generating AI content using Bulgarian pop-folk and simulated voices and faces of Bulgarian politicians, which was active during the coverage period of this report.

Screenshots taken by the authors of the report of the TikTok account @gwormzz, which produces AI-generated content of Bulgarian politicians using Bulgarian pop-folk.

Relevant Mitigation Strategy: Context-specific institutional reform aimed at developing cross-sectoral, pre-emptive readiness to combat information operations without politicisation or capture

Like Romania, Bulgaria lacks adequate institutional infrastructure to proactively monitor and respond to information operations. However, given the fragmented nature of Bulgaria's media market and citizens' disparate platform usage, a single, centralised StratCom body risks being seen by the Bulgarian public as partisan rather than competent. Because of this, Bulgarian authorities should set up a distributed network of regional StratCom nodes that link public authorities, universities, civic groups, fact-checkers and independent media. These regional notes would feed a national situational picture while operating semi-autonomously to monitor operations across platforms.

[137] *https://hssfoundation.org/wp-content/uploads/2025/09/doklad-2024-eng.pdf*

Relevant Mitigation Strategy: Investment into rapid, adaptive research programmes to keep pace with perpetrators of information operations

The Bulgarian case study demonstrates how foreign actors and their domestic proxies are able to develop and deploy new forms of coordinated inauthentic behaviour with remarkable speed and sophistication. European institutions and national authorities must now build comparable agility into their own defences. This requires investment in rapid, adaptive research initiatives capable of anticipating and countering emerging manipulation techniques as they evolve.

The EU should establish dedicated, cross-sector research programmes, modelled on the Horizon Europe framework, focused specifically on the technological, psychological and algorithmic dimensions of information warfare. These programmes must be structured for short innovation cycles that deliver operational tools and policy insights within months rather than years.

Such research efforts should be embedded within the EUDS and harmonised across member states and candidate countries. By linking researchers, regulators, civil society and media experts in a permanent network, the EU can ensure that its democratic defences remain continuously updated, evidence-based and technologically agile in the face of an accelerating threat landscape.

Conclusions & looking ahead to 2026

For Bulgaria, the drivers of algorithmic manipulation and disinformation writ large are economically and structurally embedded, presenting a diffuse, yet constant stream of vulnerabilities. Disinformation often originates on disposable, automated web domains that are monetised by advertising networks, including those with Russian links. These narratives, especially during election periods, are then amplified across social media platforms, primarily Facebook but also YouTube, Telegram and TikTok via coordinated fake accounts, paid influencers and hyper-targeted hashtag campaigns.

In Bulgaria, tactics of algorithmic manipulation can be observed that exploit local particularities of fragmented institutions and entrenched media capture. Populist and extremist parties used TikTok and influencer networks to reach younger voters, converting algorithmic popularity into real electoral gains during the June and October 2024 election cycles. Overall, the findings from our technical partner reveal a complex, adaptive disinformation ecosystem that blends genuine and inauthentic activity, underscoring Bulgaria's vulnerability to information manipulation and the urgent need for proactive, systematic countermeasures by national authorities, platforms and European institutions.

To counter such a complex threat, Bulgarian authorities must pursue a harmonised strategy

source: https://insights.manageengine.com/digital-transformation/algorithm-manipulation/

to counter disinformation and algorithmic manipulation through greater transparency, stronger regulation and institutional reform. A major roadblock that requires additional pressure from the European Commission to immediately rectify is that Bulgaria has not yet aligned its national legislation with the DSA, despite the infringement proceedings against it. Until this happens, national authorities cannot "get to work" on implementing these critical obligations.

[138] *https://digital-strategy.ec.europa.eu/en/news/commission-calls-bulgaria-comply-digital-services-act*

Other key measures include enforcing media ownership disclosure under the European Media Freedom Act (EMFA), tightening campaign finance and political advertising rules in line with the Transparency and Targeting of Political Advertising Regulation (TTPA) and developing financial forensics and ad-tech tools to dismantle the revenue networks sustaining "mushroom websites" and Russian-linked advertising platforms. The report also calls for the creation of a distributed network of regional StratCom nodes connecting authorities, civil society and independent media to monitor and respond to online manipulation.

The disinformation networks and manipulative tactics uncovered in this report are all the more concerning given that Bulgaria must hold a presidential election by the end of 2026.[139] Incumbent Rumen Radev is not able to run again due to term limits, meaning the race will be highly contested and have high stakes for both domestic and foreign policy. Voter fatigue, political apathy and skyrocketing distrust in media and other democratic institutions pose serious threats for the race, which will come amid Bulgaria's adoption of the euro[140] and the ongoing war in Ukraine–two long-standing and significant disinformation themes in the country. This will make it all the more important for European institutions and national authorities to prepare strong conditions for electoral integrity, including on online platforms, which are positioned to play a more important role than in past elections.

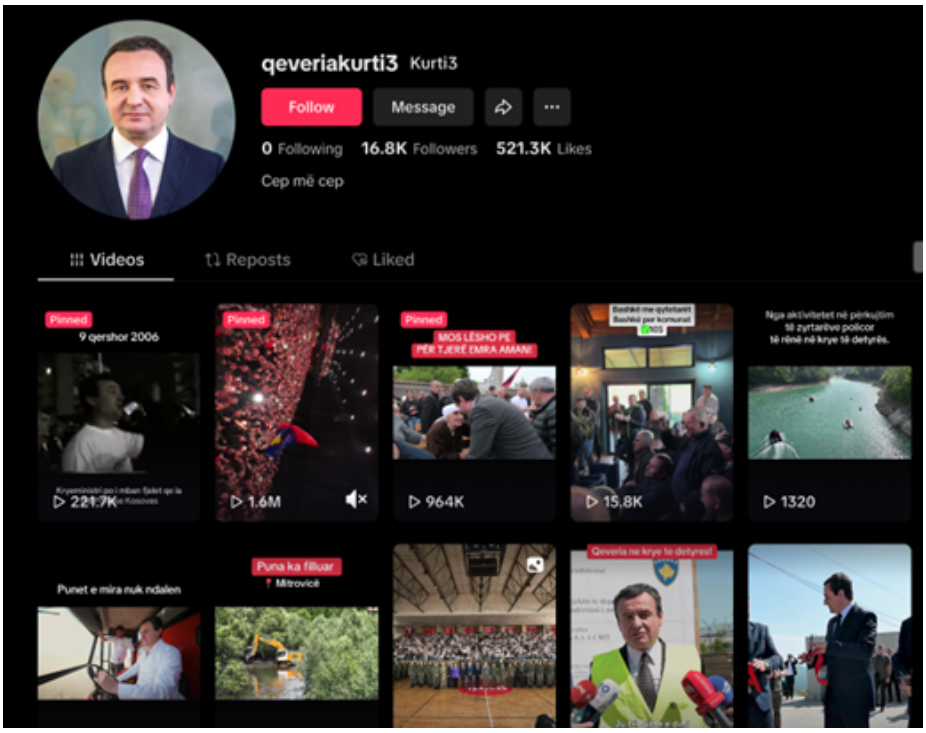
[139] *https://www.bta.bg/en/news/bulgaria/980110-cc-db-warns-of-pro-russian-campaign-to-influence-bulgaria-s-presidential-electio*

[140] *https://balkaninsight.com/2025/05/15/plebiscite-or-political-career-move-bulgarias-president-sows-euro-doubt/*

Kosovo

In a unique contribution, the report authors also briefly examined the online environment in Kosovo during the February 2025 election period, finding evidence of algorithmic manipulation similar to that observed in Romania and Bulgaria. These methods included the "Fire Hose" tactic of mass posting and commenting, synchronisation and hashtag hijacking. Much of the documented activity focused on the incumbents, the Vetëvendosje Movement (LVV) and its leader, Albin Kurti. The findings point to TikTok playing a significant role in shaping political narratives during Kosovo's parliamentary elections, especially with TikTok's being the most used social media in the country according to some estimates.[141]

Notably, all major Kosovan parties maintain an active presence on TikTok, even though the platform is formally banned in government institutions on cybersecurity grounds. As of June 28, 2024, TikTok has been blocked from all state institutions' networks and official equipment, requiring politicians to remove the app from any devices used in their official capacities. However, the prohibitions do not apply to personal networks and devices, leaving the possibility for some engagement online. Official party and leader accounts are indeed the main conduit of online narratives, which are then amplified through inauthentic networks or by genuine influencers and supporters running "theme accounts" (or some combination of the two, in order to maximise algorithmic reach).



Screenshot taken by the report authors of "theme accounts" promoting Prime Minister Albin Kurti. It is unclear whether they are run by genuine supporters or are possibly automated.

[141] *https://www.koha.net/en/tech/cloudflare-radar-tiktoku-rrjeti-social-me-i-perdoruri-ne-kosove-per-2024-n*
[142] *https://www.koha.net/en/lajmet-e-mbremjes-ktv/ndalohet-perdorimi-i-tiktok-ut-ne-pajisjet-zyrtare-e-rrjetin-shteteror-te-internetit*
[143] *https://kallxo.com/gjate/mesymja-e-kuvendit-me-influencere/?fbclid=IwY2xjawHrbupleHRuA-2FlbQIxMAABHXF7Vle3PzwYmVEvBJhWcjBbkVKmnjC0_g93Xy5t5K0qAjB6imiejinrWQ_aem_xmf-WEtr3ND5OWGbI0RA4MA*

Major political figures feature prominently across the platform, often indirectly benefiting from coordinated amplification efforts. Like in Romania and Bulgaria, content by these networks is designed for mass appeal and virality. Non-political, sport and entertainment content are often mixed with political messaging to personalise and "brand" party leaders in front of young audiences and other key voting demographics or discredit opponents.

Main active party-affiliated TikTok accounts in Kosovo

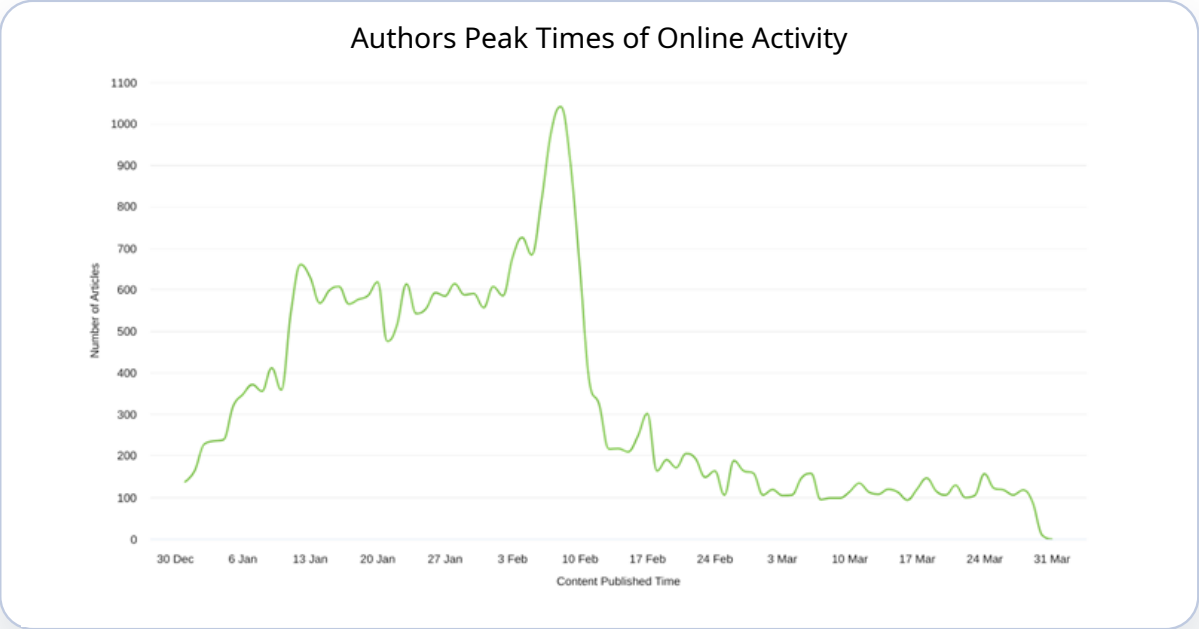
Party	Active accounts	Related hashtags
Vetëvendosje / Self-Determination Movement (LVV): incumbent ruling party with left-leaning platform.	- Arjeta Fejza (MP) - Hekuran Murati (Minister of Finance) - Fitore Pacolli (MP) - Arjeta Fejza (MP) - Faton Peci (Minister of Agriculture, GUXO party MP, in coalition with LVV)	#ALBINKURTI (16,582 mentions) #LVV (2,218 mentions)
Democratic Party of Kosovo (PDK): major opposition party with conservative platform.	- Memli Krasniqi (party leader) - Bedri Hamza (PM candidate) - Vlora Çitaku (MP) - Eliza Hoxha (MP) Valmir Klaiqi (party spokesman)	#PDK (3,310 mentions)
The Democratic League of Kosovo (LDK): centre-right party, pro-European.	- Official party account - Lumir Abdixhiku (party leader) - Hykmete Bajrami (MP) - Jehona Lushaku (MP) - Besian Mustafa (MP) - Doarsa Kica Xhelili (MP)	#LDK (6,161 mentions)
Common Front for the State coalition: comprises two smaller parties, the Alliance for the Future of Kosovo (AAK) and the Social Democratic Initiative (NISMA).	- Daut Haradinaj (MP, AAK) - Fatmir Limaj (party leader, NISMA) - Bekë Berisha (MP, AAK) - Time Kadriaj (MP, AAK)	

The most striking method of algorithmic amplification uncovered was the "Fire Hose" tactic, in which extremely high volumes of posts were generated by a few—or even single—actors in order to flood TikTok's recommendation system. For example, one account, @hamzahatika46, published over 18,000 videos during the campaign, accumulating more than 13 million engagements.

Source	Influencer	Posts	Engagement	Engagement per post
	@hamzahatika46	18,065	13,221,036	732
	shqiptarivertete @shqiptarivertete	259	487,894	1,884
	Tokë IliroDardane @toke.ilirodardane	274	334,265	1,220
	B7 @batmank77	22	334,227	15,192
	Kurti3 @qeveriakurti3	20	318,486	15,924

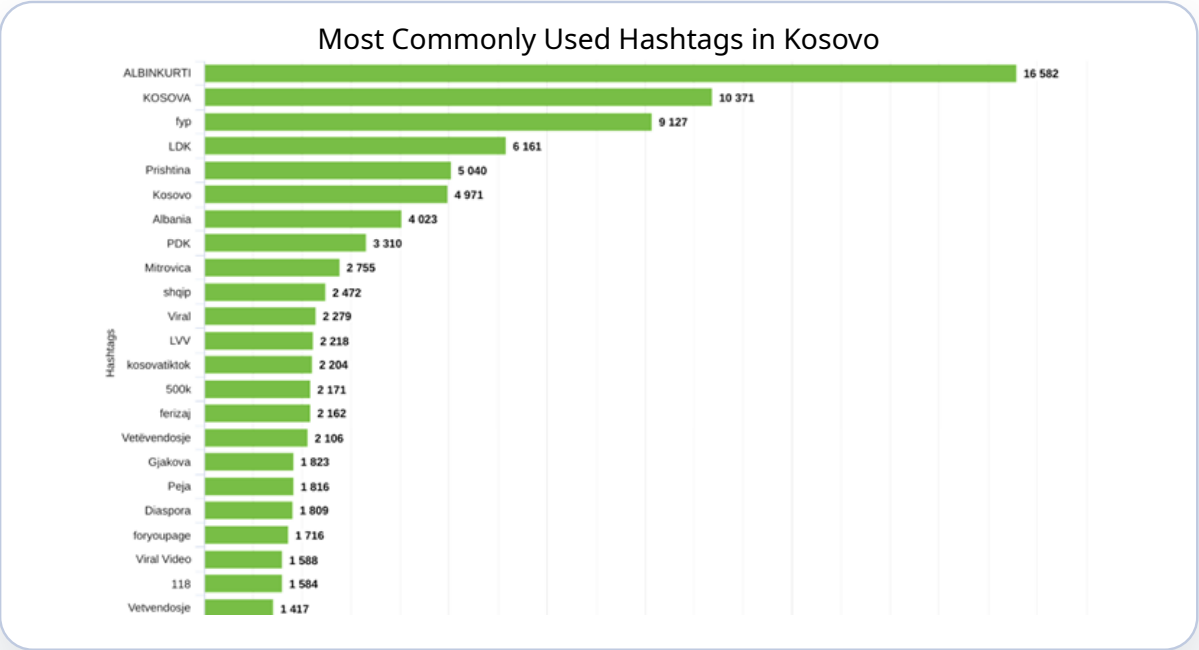
Screenshot of Sensika data taken by the report authors showing top influencers in Kosovo during the monitoring period.

Such posting intensity suggests automated or semi-automated coordination designed to maximise visibility, overwhelm organic content and dominate discourse. Spikes in coordinated activity, particularly on or around February 8–10, indicate an orchestrated effort to shape online sentiment and visibility during a critical political window.



Screenshot of Sensika data taken by the report authors showing peak times of online activity during the monitoring period.

Hashtag analysis demonstrates extensive manipulation of both political, generic and geographic hashtags, such as combining #lvv or #ldk with #fyp, #viral and #kosova, to expose political content to users not actively following political topics. There was also evidence of hashtag hijacking, with rival party tags being co-opted to circulate critical or misleading content about opponents.



Screenshot of Sensika data taken by the report authors showing the most commonly used hashtags in Kosovo during the monitoring period.

Relevant mitigation strategy: Inclusion of candidate and prospective candidate countries into democracy defence architecture

TikTok's algorithmic dynamics make it particularly susceptible to manipulation in small digital ecosystems such as Kosovo's, as the findings here clearly show. The nature of online information operations as fundamentally borderless poses European-wide threats to democracy and security, underscoring the urgent need for Brussels to look for ways to integrate current and prospective candidate countries into its democracy defence architecture. Concretely, this could include integrating Kosovo and similar "front line" countries into cross-border monitoring and research initiatives; supporting country- and region-specific trainings, tool kits and other forms of in-kind support to credible media to respond to these threats in Europe's most sensitive security contexts; reinvigorating media financing in these contexts more generally; and ensuring partners from these contexts are involved in media and digital literacy education that protects against inadvertent participation in algorithmic manipulation.

The 2025 parliamentary elections in Kosovo were the first major elections to take place after an armed group of Serbs attacked Kosovo Police in Banjska, located in the Serb-majority north of the country, in September 2023. The attack was the latest in a string of violent altercations in this part of Kosovo, such as widely-covered clashes between Serb protesters and NATO-led KFOR troops earlier that year in May. The confrontation in Banjska resulted in the death of Kosovo police sergeant Afrim Bunjaku and three of the attackers. Milan Radoičić, then the vice president of the Serbian List, the largest political party representing Kosovo Serbs, later claimed responsibility for the attack.

The tragic incident was not only a harsh reminder of the fragile security situation in Kosovo, especially in northern municipalities, it also exposed the country to a barrage of disinformation about the nature of the attack. This wave of disinformation, according to local independent media and expert analysis, appeared to originate from Serbian and Russian sources and specifically targeted Kosovo's security institutions. Narratives surrounding these events continued to be highly prevalent throughout the 2025 election cycle, as this analysis confirmed.

Algorithmic manipulation, including the tactics observed during Kosovo's 2025 election, therefore not only presents problems for information integrity, it also poses direct security risks. Such manipulation deepens ethnic mistrust, weakens confidence in democratic institutions and risks spillover into offline tensions. The erosion of media credibility–and declining media freedom more generally–only compound these threats, as citizens lose reliable sources of information and become more vulnerable to extremist or foreign-sponsored narratives. In this context, online disinformation and polarisation function as tools of strategic destabilisation, transforming the digital domain into a front line of Kosovo's national security challenge, with conflict risks for all of Europe.

[144] *https://www.dw.com/en/kosovo-monastery-siege-ends-with-4-dead/a-66909234*
[145] *https://www.rferl.org/a/northern-kosovo-ethnic-albanian-mayors-kfor-serbs/32432330.html*
[146] *https://balkaninsight.com/2024/09/24/a-year-after-banjska-attack-kosovo-indictment-chronicles-serb-land-grab-plot/*
[147] *https://www.ndi.org/sites/default/files/INFORMATION%20DISORDERS%20IN%20KOSOVO%20-%202023-compressed_0.pdf*
[148] *https://prishtinainsight.com/kosovo-security-sector-becomes-target-of-disinformation-mag/*
[149] *https://prishtinainsight.com/kosovos-pm-accuses-serbia-of-interfering-in-parliamentary-elections/*
[150] *https://balkaninsight.com/2025/04/02/hate-speech-marred-kosovos-2025-election-birn-report-finds/*
[151] *https://www.rcc.int/download/docs/BB2024-PO.pdf/c29cfed20c3776d280077cdfc2617abc.pdf*

Conclusions & Recommendations

This report has shown that algorithmically-driven influence operations are no longer isolated incidents but rather part of a systemic and evolving threat to democratic integrity across Europe. The case studies of Romania and Bulgaria illustrate two distinct but interconnected faces of this challenge: one acute and destabilizing, the other diffuse and endemic. The additional brief on Kosovo underscores the borderless nature of these challenges, as well as the security risks that can come from such manipulation if left unchecked. Together, the three case studies highlight how underregulated digital platforms, weak financial transparency laws within and across borders and long-standing institutional weaknesses can converge to create an environment conducive to digital manipulation, foreign interference and wide-reaching destabilisation.

The 2024–2025 presidential elections in Romania are now a landmark case in modern information warfare. Georgescu's manipulation operation relied on hybrid tactics: paid influencer marketing disguised as apolitical content, synchronised use of hashtags and comment "bombing" by bot networks. Over 25,000 compromised TikTok accounts were found to have artificially amplified the campaign of pro-Russian candidate Călin Georgescu, transforming online virality into genuine political momentum.

The operation exploited both platform vulnerabilities and institutional blind spots. TikTok's engagement-driven recommender systems rewarded coordinated behaviour instead of flagging it, while Romanian authorities lacked clear escalation protocols, effective inter-agency coordination and transparent public communication to pre-empt such manipulation. Fragmented governance between national regulators, opaque campaign financing and weak enforcement of the Digital Services Act (DSA) allowed disinformation networks to operate freely. Although both the Romanian government, the European Commission, the platforms, and civic-minded media took corrective measures, these steps were largely reactive and therefore insufficient. Anticipatory, cross-sectoral coordination, anchored in the European Democracy Shield (EUDS), has the potential to prevent future algorithmic interference from escalating to the level witnessed in Romania.

The Bulgarian case presents a different but equally troubling picture. Rather than a single, large-scale operation, Bulgaria's 2024 elections revealed a persistent ecosystem of algorithmic manipulation, rooted in opaque ownership structures, automated "mushroom websites," and financially incentivised disinformation networks. These disposable online domains, monetised through advertising networks such as the Russian-linked AdNow, continuously generate clickbait and false narratives that can migrate across Facebook, YouTube, Telegram and TikTok. By exploiting the virality mechanisms of TikTok and the targeting precision of Facebook, political parties and their affiliates can transform algorithmic visibility into measurable–though minor–electoral success.

Bulgaria's overlapping political crises, weak regulatory enforcement and high levels of media capture have allowed disinformation to become economically embedded and normalised in both online and traditional media. To address this, the report authors call for robust media ownership transparency under the European Media Freedom Act (EMFA), tightened campaign financing and advertising disclosure aligned with the Regulation on the Transparency and Targeting of Political Advertising (TTPA) and the creation of a distributed network of regional StratCom nodes that can resist politicisation and capture. Bulgaria would also benefit from the proposed interventions in Romania, as would Kosovo, as all of the recommendations in this report are applicable across Europe.

Given that Kosovo faces similar online threats as Romania and Bulgaria, albeit in a weaker regulatory and security environment, the lesson is clear: algorithmic manipulation and coordinated disinformation are not isolated national problems but structural weaknesses in Europe's information ecosystem. Platforms remain reactive rather than preventive, focusing on post-crisis account removals rather than risk mitigation. National regulators act in silos, often constrained by limited capacity or political capture. Credible media and civic actors, though vital to detection and awareness, lack sustained institutional support. There is a critical policy gap between legislation and implementation: the DSA

provides the legal foundation for platform accountability, but enforcement remains reactive overall and uneven across member states.

The EUDS, if fully realized, could bridge these divides. By connecting legal, technical and civic responses, the EUDS can create a coherent, anticipatory defence architecture for European democracy. To operationalise this vision, the report authors recommend, in all European countries:

Strengthening DSA enforcement through clear, binding guidance on systemic risk mitigation, political advertising transparency and content moderation during elections;

Situating the European Democracy Shield as the EU's central mechanism for real-time detection and systematic response to influence operations;

Enforcing full transparency in media ownership and campaign financing under the EMFA and TTPA, targeting both domestic and cross-border funding streams;

Protecting the independence of public-interest media while also increasing in-kind and other support for credible media to train journalists and play a central role in systemic disinformation-fighting efforts both on and offline;

Investing in EU-backed digital forensics and ad-tech disruption tools to trace and dismantle the economic underpinnings of disinformation networks, including Russian-linked advertising infrastructures;

Supporting digital literacy and pre-bunking initiatives, especially among young voters, to enhance civic resilience to (and inadvertent participation in) algorithmic disinformation; and

Establishing independent, depoliticised national and regional StratCom networks, integrated into the EUDS, to promote information sharing, rapid response and trust-based cooperation among institutions, civil society and media actors.

Summary of recommendations by actor

European Commission	National	Platforms
Invest in public awareness campaigns and media / digital literacy campaigns.	Invest in public awareness campaigns and media / digital literacy campaigns.	Work with relevant European and government actors to devise clear systematic risk mitigation strategies under the DSA, including the publishing of an effective and transparent advertising repository for cross-sector monitoring efforts.
Provide clearer guidelines to national authorities and platforms on mitigating against election-related risks under the DSA, including for non-VLOPs like messaging platforms.	Tighten campaign financing regulations, including decreasing the size of state subsidies for party campaign materials, as well as improving the monitoring and verification of campaign expenditures	Work with relevant European actors to develop metrics for performance on coordination / inauthenticity detection / removal, which can feed into more frequent and more accessible progress reporting on prevention and takedown efforts.
Create specialised teams under DG CONNECT to ensure platform accountability, linked with business incentives.	Improved anti-money laundering measures such as through FATF recommendations	Update policies and enforcement processes related to political advertising, including developing easy and effective tools for creators to self-disclose paid or sponsored content.
Support, work with and incentivise national authorities to meet their DSA obligations, especially those related to inter-institutional coordination.	Expand the powers of electoral authorities to better investigate and sanction campaign finance violations.	With national authorities, experts and civic actors, develop transparent content and account removal guidelines.
Assist in convening multi-stakeholder consultation for national authorities.	Ensure the clear labelling of paid and/or campaign content online including through appropriate sanctioning of violations	Deploy local "trusted flaggers" early and help launch pre-bunking campaigns.
Ensure the implementation of the TTPA.	Establish StratCom body/bodies to lead in the proactive monitoring of the information space before elections.	
Require platforms to develop content and account removal guidelines for election related content that are also socialized with local stakeholders.	Develop transparent content and account removal guidelines via a multi-stakeholder consultative process and pursue a compliance architecture aligned with international best practice.	
Issue additional compliance guidelines related to content and account removal criteria specifically for cases of cross-border entities.	Support civic society to act as platform "trusted flaggers" and leaders in pre-bunking campaigns.	
Invest into rapid, adaptive research programmes to keep pace with perpetrators of information operations, involving cross-sector stakeholders and national- and regional-level experts.	Lead in the creation of socialised emergency protocols once influence operations are detected during electoral periods.	
Revamp financing and in-kind support for independent media specifically targeting areas of digital transformation, effective online communication skills and other disinformation-fighting capabilities.	Develop and commission post-election technical assessments and other civic monitoring tools for inter- and post-election learning.	

About the Authors

About the Balkan Free Media Initiative.

The Balkan Free Media Initiative (BFMI) is a Brussels-based, independent civil society organisation founded in April 2021 to address the gap in accountability and advocacy on media freedom issues in Southeastern Europe. BFMI monitors developments across the Balkans and informs Western political audiences about the threats to democracy and peace due to the declining information environment. It focuses on overlooked structural issues and market manipulation of the media sector across the region.

About Sensika.

Sensika Technologies is a Sofia-based company established in 2012 that develops AI-driven media monitoring and analysis solutions for research on information ecosystems and disinformation. Its Software-as-a-Service (SaaS) platform provides real-time, 360° monitoring across online news, social media, broadcast and print. Combining automated analytics with human expertise and a continuously updated, categorised source catalogue, Sensika enables crisis monitoring, tracking of campaign development, disinformation and reputation monitoring. The platform allows to detect and map false narratives, coordinated networks and influence operations, generating structured, data-driven insights that enhance early warning and evidence-based decision-making.

Acknowledgements

The authors are grateful to the many media experts and journalists who contributed their time and knowledge to the preparation of the report. Die Morina van Uijtregt provided invaluable assistance with the Kosovo section. Serban Barbu and Nikola Tulechki reviewed and fact checked the chapters on Romania and Bulgaria. BFMI's advisory board and staff deserve special thanks. Peter Horrocks, Mark Nelson and Teresa Ribeiro were essential to the report's conception and development. The research for this report was prepared by BFMI Research & Communications Manager, Alexandra Karppi and BFMI Co-Founder & Director, Antoinette Nikolova. Its publication and promotion was supported by Tanja Albreht, Vanesa Valcheva and Mano Manov.

SENSIKA

Appendix I:

Glossary of Acronyms & Abbreviations

AAK - the Alliance for the Future of Kosovo
API - Application Programming Interface
AUR - Union of Romanians
DG CONNECT - Directorate-General for Communications Networks, Content and Technology
DPS-NN - Movement for Rights and Freedoms-New Beginning
DSA - Digital Services Act
DSC - Digital Services Coordinator
ECNE - European Cooperation Network on Elections
EMFA - European Media Freedom Act
EUDS - European Democracy Shield
FATF - Financial Action Task Force
FIMI - Foreign Information Manipulation and Interference
GERB - Citizens for European Development of Bulgaria
Greatness - Velichie
ITN - There Is Such a People
LDK - The Democratic League of Kosovo
LVV - Vetëvendosje Movement (Self-Determination Movement)
MECH - Morality, Unity, Honour
NISMA - the Social Democratic Initiative
PDK - Democratic Party of Kosovo
PEA - The Permanent Electoral Authority
Revival - Vazrazhdane
StratCom - Strategic Communications
TTPA - Regulation on the Transparency and Targeting of Political Advertising
VLOPS - Very Large Online Platforms

Appendix II:

Methodology for Detecting Manipulation on Tiktok

Objective and Scope

This methodology aims to identify TikTok videos with potentially inauthentic engagement—artificially boosted through paid services or coordinated campaigns. The focus is on content disseminated during electoral periods (June and October 2024).

1. Network Detection (Entry Point)

Before analyzing individual videos, we must understand the **network of accounts** amplifying the content:

- Start from a **key hashtag (**e.g., #меч, #рудигела, #ивелинмихайлов).
- Identify which influencers repeatedly appear under that hashtag.
- Check **video reposts and stitches** across accounts.
- Map the most **active amplifiers** and their interconnections.
- Identify the **biggest influencers** and isolate suspicious videos by metrics.
- Expand the network by checking **links in bios** (Facebook, YouTube, Telegram, Instagram, websites) for cross-platform coordination.

2. Indicators of Manipulation

2.1 Low Engagement Rate (ER) with High Reach

- **Formula (Exolyt):**
  ER=(Likes+Comments+Shares)/Views
- **Risk zones (Exolyt):**
  - 🟢 Normal: >3%
  - 🟡 Low but acceptable: 2–3%
  - 🟠 Suspicious: 1–2%
  - 🔴 Highly suspicious: <1%
- **Benchmarks:**
  - Average TikTok ER ≈ 3.8–4.2% (Socialinsider, 2024)
  - Median TikTok ER ≈ 4.07% (Brandwatch, 2025)
  - Small accounts often 5–9% ER; large accounts rarely below 2% (Emplicit, 2025)
  - For videos with large reach, ER <2% is abnormal; <1% strongly suggests manipulation.
- **Data Sources:**
  - **Exolyt (trial version available):** automatic ER calculation per video
  - **Sensika:** raw data (likes, comments, shares, views) can be used for manual ER calculation

2.2 Burst Views (Sudden Surges in Views) – Future Capability

Definition: Sharp spikes in views within 24–48h, without proportional growth in likes, comments, or shares.

- Useful for identifying **purchased engagement** (NATO StratCom COE, 2024; Nevado-Catalán et al., 2022).
- At this stage, **we do not have time-series data on view accumulation,** so this indicator cannot yet be applied.
- Should be activated once platforms or third-party tools provide **temporal breakdowns of views/likes/comments.**

2.3 Fire Hose Pattern (Mass Reposting of Variations)

Definition: Nearly identical videos (small changes in soundtrack, editing, captions) are posted by multiple accounts.

Effect: Algorithm treats each as "new" -> amplifies reach, creates informational noise.

- Matches RAND's "Firehose of Falsehood" propaganda model (Paul & Matthews, 2016).

2.4 Metric Imbalances and Fake Engagement Signs

Description: Inconsistent or unnatural metrics, often linked to fake engagement tactics.

- Purchased followers/likes, engagement pods, bots, cloned content (Stack Influence, 2025).
- **Red flags:**
  - Low engagement despite high reach
  - Generic/repeated comments
  - Sudden unexplained audience spikes
  - Imbalance: many likes but very few comments/shares

2.5 Platform Policies

TikTok bans manipulative behaviour such as fake views, likes, followers and coordinated inauthentic activity.

- TikTok Newsroom (2024): removed over **36 billion fake likes** and **700 million fake accounts** in 2024.

3. Application in Electoral Context

- Videos with **ER <0.02 (2%),** especially <0.01, are flagged.
- Burst view patterns (future capability) will allow stronger detection of paid boosting near election dates.
- Fire hose clusters suggest coordinated campaigns.
- Metric imbalances reinforce suspicion when combined with ER and network analysis.

4. Indicators of Manipulation on TikTok (Summary Table)

Indicator	Definition / Threshold	Evidence / Source	Status
Engagement Rate (ER)	ER = (Likes + Comments + Shares) / Views. Suspicious: <2%, Highly suspicious: <1%	Exolyt Calculator (2024, trial available). Sensika raw data. Benchmarks: Socialinsider (2024), Brandwatch (2025), Emplicit (2025)	Active
Burst Views	Sudden spike in views over 24–48h, without matching likes/comments/shares	NATO StratCom COE (2024); Nevado-Catalán et al., 2022	Future Capability
Fire Hose Pattern	Multiple accounts post near-identical videos (minor variations)	RAND, Paul & Matthews (2016)	Active
Metric Imbalances	Many views/likes but very few comments/shares; sudden unexplained spikes; generic comments	Stack Influence (2025)	Active
Platform Policies	TikTok bans fake views, likes, followers, coordinated inauthentic behaviour	TikTok Newsroom (2024)	Active

5. References

- **Exolyt.** TikTok Engagement Rate Calculator (2024).
- **Socialinsider.** Social Media Benchmarks 2024.
- **Brandwatch.** What is a Good Engagement Rate on TikTok? (2025).
- **RivalIQ.** TikTok Benchmark Report 2024.
- **Emplicit.** TikTok Engagement Rate Benchmarks 2025.
- **NATO StratCom COE.** Social Media Manipulation for Sale (2024).
- **Nevado-Catalán, E. et al.** *An analysis of fake social media engagement services.* Computers & Security (2022).
- **Paul, C. & Matthews, M.** *The Russian "Firehose of Falsehood" Propaganda Model.* RAND (2016).
- **Stack Influence.** *Fake Engagement on TikTok: What It Is and How to Spot Fake TikTok Influencers* (2025).
- **TikTok.** *How TikTok counters deceptive behaviour.* Newsroom (2024).

TikTok Manipulation Detection Checklist

Step 1. Build the Network

- [ ] Start with a **key hashtag** (e.g., #меч, #рудигела, #ивелинмихайлов).
- [ ] List all **active accounts** using it.
- [ ] Identify **main influencers** (largest follower base + highest reach).
- [ ] Map **reposts and stitches** of the same videos across accounts.
- [ ] Collect links from bios **(FB, YouTube, Telegram, Instagram, websites)** for cross-platform expansion.

Step 2. Engagement Rate (ER)

- [ ] Collect data (likes, comments, shares, views) -> from E**xolyt trial** or **Sensika raw export.**
- [ ] Calculate: ER=(Likes+Comments+Shares)/Views
- [ ] Compare with thresholds:
  - 🟢 Normal: >3%
  - 🟡 Low but acceptable: 2–3%
  - 🟠 Suspicious: 1–2%
  - 🔴 Highly suspicious: <1%

Step 3. Burst Views (Future Capability)

- [ ] Look for sudden view spikes within 24–48h.
- [ ] Requires **time-series view data** (not currently available).
- [ ] Mark as "future indicator" for integration when platforms allow.

Step 4. Fire Hose Pattern

- [ ] Search for **nearly identical videos** with small changes (music, editing, captions).
- [ ] Note if multiple accounts post them within a short time.
- [ ] Flag as **coordinated amplification.**

Step 5. Metric Imbalances

- [ ] Cross-check metrics for inconsistencies:
  - [ ] High views + very low likes/comments
  - [ ] Many likes but almost no shares
  - [ ] Generic / template comments
  - [ ] Sudden unexplained audience spikes
    - [ ] If multiple red flags appear -> mark as **likely manipulation.**

Step 6. Policy & Context Check

- [ ] Verify alignment with **TikTok's bans** on fake engagement.
- [ ] Place anomalies in **electoral context** (±7 days around election events).

Decision Rule:

- If ER <2%, or if Fire Hose pattern + imbalanced metrics are detected -> flag video as manipulated or suspicious.
- If combined with cross-platform amplification -> escalate to full case study.

BFMI

BALKAN FREE MEDIA INITIATIVE

Tackling TikTokcracy in the Balkans
Brussels, November 2025

BALKANFREEMEDIA.ORG