POLICY BRIEF No. 234 May 2026

The government crisis and manipulation on TikTok.

A monitoring report April–May 2026

Authors: **Madalina Voinea**, Digital Analyst | **Monirul Hassan**, Independent Researcher, Computer Science | **Vlad Adamescu**, Political Scientist

Contents

2.1 Trends in post volume **6**

2.2 Coordination clusters between accounts **6**

Example of operational alignment 8

2.3 Analysis of comments **8**

2.4 Analysis of followers of main accounts **10**

2.5 Key topics and the real-world impact of these narratives **12**

3.1 Use of female accounts (use of women's profiles) **15**

3.2 Geția content **16**

5.1 National regulations for the domestic non-authentic industry **1G**

What is missing from national regulations? 19

Clear rules for political actors online 19

Revision of national regulations on the funding of promotional campaigns 19

5.2 STRATCOM – Building civil society capacity for strategic communication in Romania **20**

1. Context: The political crisis in Romania, the digital media landscape and inauthentic campaigns as information pollution

In a period of political crisis, Romanians' TikTok feed is a battlefield of information. We analysed **23,599 viral political videos** from the start of the year. Of these, between 1 April and 11 May 2026 alone, **the videos monitored generated 101.9 million views, 829,000 shares and**
68,400 comments. 52% of the comments were clusters of duplicate posts. **Of the 267,799 followers of the accounts that produced this content, 53.1% were empty accounts with no videos posted. Are we talking about real people, concerned citizens, patriots?** Our data suggests the continuous presence of amplification networks that artificially keep the conversation at fever pitch precisely at the moments when the public is most vulnerable. In this context, we ask ourselves how we can determine who was there first: the inauthentic accounts or the genuine supporters? More importantly, who is accountable in a democracy for the manipulation of information reaching citizens?

Romania is undergoing a severe government crisis after the ruling coalition collapsed following the vote on the motion of no confidence in Parliament. The economic situation is steadily deteriorating; political uncertainty, inflation of over 10 per cent and the geopolitical situation at the border have created an information landscape rife with uncertainty, discontent and opportunities for the political exploitation of these realities.

The situation in Romania is no exception; rather, it is part of a global trend of inaction on the part of major social media platforms which, in the absence of safety mechanisms to guarantee the integrity of the services they provide, allow these types of campaigns to infiltrate people's feeds. In the NATO Strategic Communications Centre of Excellence report, 'Beyond Spam Bots', published in April 2026[1] *, artificial amplification on social media via customised systems based on LLMs (ChatGPT, Claude and others) is the main concern regarding the manipulation of online conversations.*

[1] Chia Tee Hiang, J., and G. Bergmanis-Korāts, *Beyond Spam Bots: The Rise of AI-Powered Disinformation Machines and the Imperative for Strategic Response* (Riga: NATO Strategic Communications Centre of Excellence, 2026), https://stratcomcoe.org/publications/beyond-spam-bots-the-rise-of-ai-powered-disinformation-machines-and-the-imperative-for-strategic-response/342.

Capability	First generation (2016–2020)	AI-enabled (2024–)
Content generation	Template-based, repetitive, easily identified	Context-aware, persuasive, indistinguishable from human
Persona management	Static fake accounts with thin backstories	Dynamic synthetic identities with adaptive psychological profiles
Targeting	Broad demographic categories	Psychological vulnerability mapping; real-time sentiment analysis
Adaptation	Manual adjustment based on observed results	Automated feedback loops; self-optimising tactics
Scale	Labour-intensive; human operators required	Industrial-scale automation with minimal oversight

Source: NATO Strategic Communications Centre of Excellence, Beyond Spam Bots: The Rise of AI-Powered Disinformation Machines and the Imperative for Strategic Response, Riga, April 2026

With the advent of LLMs, online disinformation campaigns have become accessible to any malicious actor seeking to spread misinformation in order to promote their own agenda, at minimal cost but with maximum efficiency. This efficiency translates into the mass creation of tens of thousands of fake accounts that mimic human behaviour beyond what we can detect purely visually. Whereas before LLMs we observed lazy, repetitive bot campaigns with easily observable coordination factors, we now see the mimicry of human behaviour within a far more complex system. What signals remain? Anomalies in interactions on a specific topic from suspicious accounts, the invasion of digital space by accounts that intensify their activity in a coordinated manner, promoting potentially inauthentic posting patterns (same times, high volume, same messages). However, we are talking about incomplete and constantly changing definitions; this is precisely why we consider the definition from the latest EEAS report to be relevant to the Romanian phenomenon.

> ***Coordinated Inauthentic Behaviour (CIB)*** *– Involves organised, deliberate and manipulative efforts to mislead the public through the use of multiple fake or inauthentic accounts. Generally, this includes networks of accounts and pages that collaborate to spread certain messages or carry out specific actions, whilst concealing their true nature. CIB operations rely on the extensive use of manipulative tactics and techniques.*
>
> *Source: European External Action Service (EEAS), 4th Report on Threats to Information Security, 2026.*[2]

[2] European External Action Service (EEAS), *4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards* (Brussels: EEAS, March 2026), https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf.

Who should take action? European regulations have established a response framework through the Digital Services Act (DSA), which imposes ongoing obligations on Very Large Online Platforms (VLOPs, e.g. Meta, TikTok) to assess and mitigate systemic risks. According to Article 34 of the DSA, a government crisis on the scale of that in Romania explicitly falls within the category of systemic risks, given its negative effects on civic discourse, electoral processes and public security. Furthermore, the Code of Conduct on Disinformation (2025), incorporated into the DSA, explicitly prohibits manipulative behaviour, including the creation of fake accounts, amplification via bots and non-transparent promotion through influencers. However, we note that these obligations are not consistently upheld. Whilst during the elections the platforms attempted to maintain the appearance of safeguards against artificial traffic, we now observe a rather passive stance, at least in the case of this latest political crisis.

The responsibility for safeguarding the services they provide within the European Union in the face of this new wave of coordinated disinformation campaigns lies, first and foremost, with the major platforms. However, we believe that action is also needed at national level.

Beyond the obligations of the platforms, the response to information pollution requires action at a societal level. **In this report, we propose three complementary approaches:**

- **the regulation of online political advertising**, which should explicitly include a ban on the use of campaigns containing inauthentic content by marketing companies contracted by Romanian political parties. Such regulation could be accompanied by a Code of Conduct for parties in the online environment.
- **Enhancing the civil sector's capacity for strategic communication** by establishing a Romanian STRATCOM. This does not involve replicating models from France, Sweden, Norway or Moldova, but rather, first and foremost, conducting studies on the Romanian information landscape, consumption habits and vulnerabilities, in collaboration with experts from universities and civil society.
- **A clear distinction must be drawn** between legitimate forms of user coordination in the online environment – such as coordinated campaigns by citizens to support a politician, information campaigns, and organic political expression campaigns – and inauthentic coordinated campaigns.

The lesson missed from the 2024–2025 elections regarding the online environment is that inauthentic domestic interference, alongside external interference—whether confirmed or not—has not disappeared. Both operate 24/7, even outside election campaigns, to polarise Romanians. The question is not whether Romania needs a coordinated response, but whether the Romanian state will wish to build it transparently, in partnership with civil society, experts, the press and universities, or whether it will, as is customary, leave it entirely to the security services, without adequate communication with society.

2. Analysis of 23,599 videos, 68,000 comments and 267,286 accounts, between 11 January and 11 May

2.1 Trends in posting volume

Our analysis reveals a sudden surge in posting activity during the government crisis of April–May 2026. Total video production rose steadily from January, before accelerating sharply in April and peaking at nearly 4,000 videos over a 14-day period, a level almost four times higher than that observed at the start of the year. Daily activity patterns show a steady rise and a peak between 1 and 5 May, leading up to the no-confidence motion, with repeated peaks exceeding 400–500 videos per day.

The number of posts published by the 49 source accounts has been steadily increasing since January. From 57 videos posted per day, by April they were posting an average of 246 videos per day, a pace that continued throughout April. We observed **a fourfold increase in posting activity across these accounts** between April and May.

Two accounts stand out, having likely been created or converted into political accounts in 2026:

- breakingtiktok78, whose first post appeared in March 2026, posted 526 videos in its first month, then 2,270 in April, accumulating 32 million views in less than two months on exclusively pro-AUR, anti-government political content.
- live1977 appeared on 1 April 2026 and posted 788 videos in 40 days, reaching 7 million views.

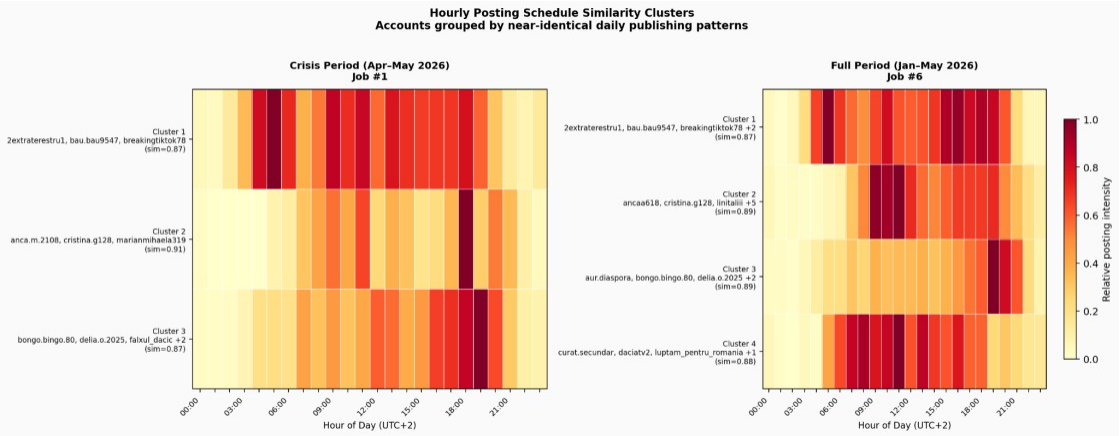
Both accounts started from scratch and operated on a large scale, with dozens of posts a day and millions of views within a few weeks, focusing on manipulated news stories against the SAFE programme, manipulated news about President Nicușor Dan, former Prime Minister Ilie Bolojan, and pro-Călin Georgescu and AUR content.

These are not the only accounts exhibiting such behaviour: we analysed all accounts in the network that, from their very first activity, posted exclusively about politics. For example:

- **romaniaazi2 joined on 2 April and posted 92 videos in 39 days,**
- **tiktoklivia00 posted their first video on 19 April and has posted 280 videos in 22 days,**
- **alapacino_omega has 272 videos in 15 days starting from 26 April.**

It is important to note that these accounts did not transition from general content to political content. Their sole political content, right from the very first post, has been exclusively against the former Ilie Bolojan government and against Nicusor Dan.

2.2 Coordination clusters between accounts

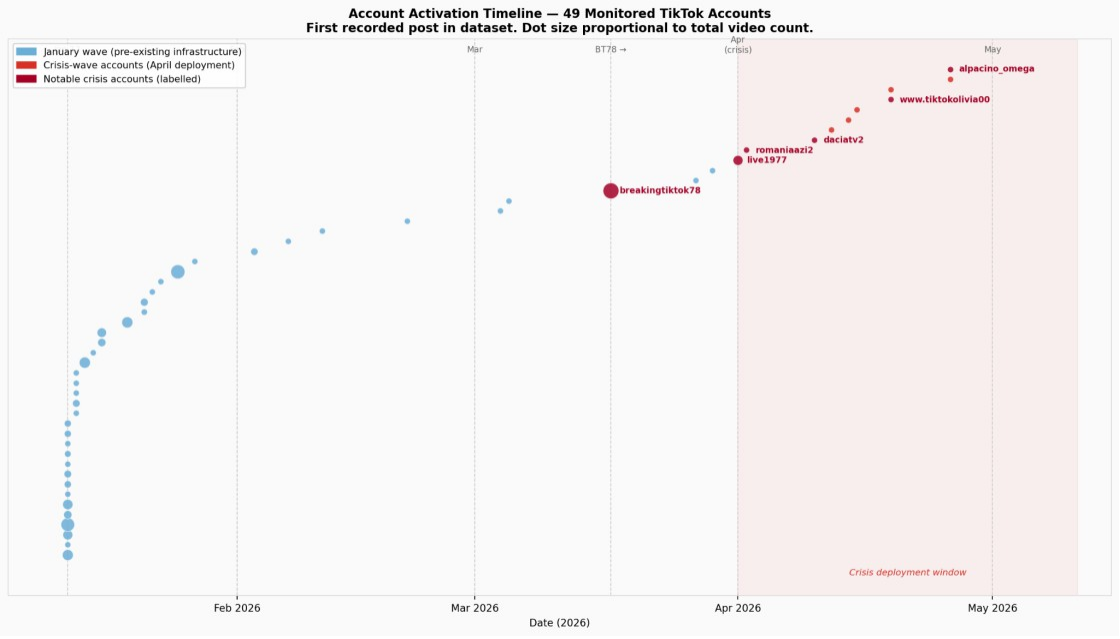


How does the network of these accounts function? We analysed the daily posting schedule of all 49 main accounts across the entire period from January to May 2026 and identified almost identical posting time slots. Three such groups emerged during the crisis period of April–May:

- one group consists of anca.m.222108, cristina.g128 and mmmarianmihaela319, all of whom concentrated their activity between 18:00 and 20:00;
- a second consists of bongo.bingo.80, delia.o.2025, falxul_dacic, simion.c68 and tnt5559, all active during a shared afternoon slot;
- a third links 2extraterestru1, bau.bau9547 and breakingtiktok78 around an early morning distribution.

We extended the analysis to the full five-month dataset; the same clusters persist and expand, with additional accounts being added. Among these, luptam_pentru_romania, romaniaazzi2 and stellabella103 maintained the same modus operandi between January and May.

The three groups from the crisis period have clear posting patterns: distribution in the morning and afternoon, and a peak in the evening between 18:00 and 20:00.



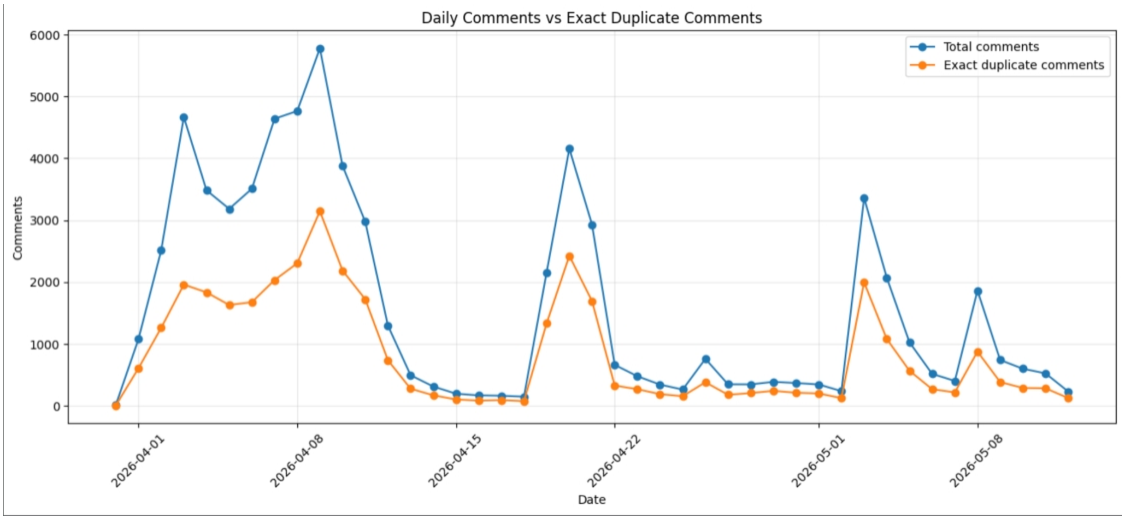
The fact that this posting schedule remains constant over five consecutive months is a key indicator. Citizens and journalists covering political events might

synchronise their posting times on a single busy day, but we believe that the maintenance of an almost identical hourly distribution every day for five months by anonymous accounts, many of which were activated at the start of the year, indicates a possible operational alignment.

Example of operational alignment

At the pair level, an analysis of post timestamps reveals a hub-and-spoke structure[3]in which certain accounts act as dedicated amplifiers for others. Linitaliii posts within five minutes of luptam_pentru_romania in 11% of its posts, and the pair anca.mm.2108 and cristina.g128, analysed in detail in section 3, post within thirty minutes of one another in 44% of cases. Such near-instantaneous synchronisation on a large scale does not correspond to manual behaviour, but indicates the existence of tools operating simultaneously across multiple accounts.

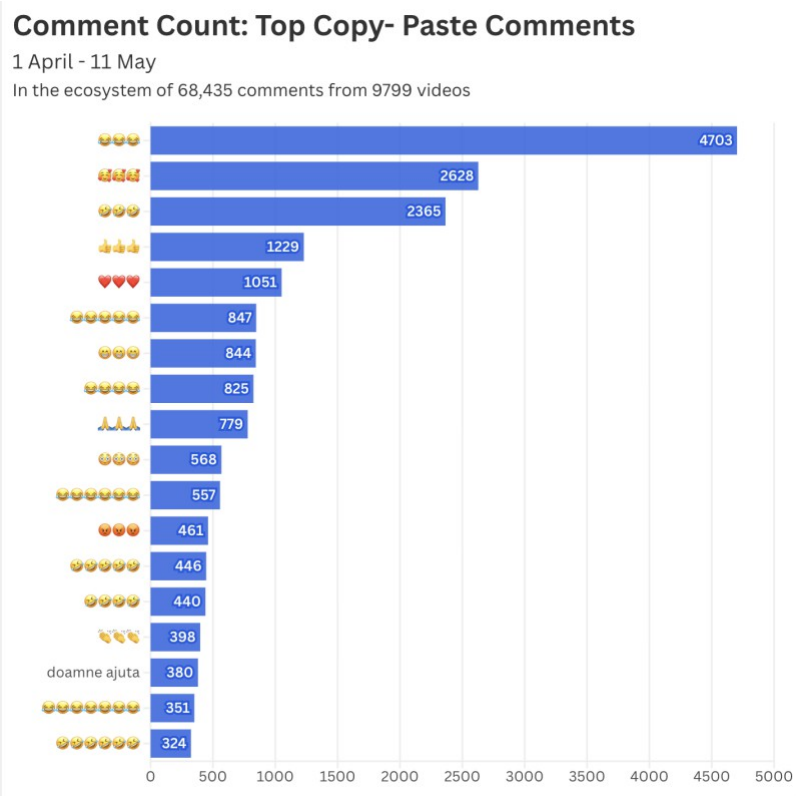
2.3 Analysis of comments



Most of the comments analysed consist of a repetitive sequence of emojis. We limited our analysis to comments repeated at least five times and identified 36,000 comments. Approximately 47% of these are duplicate comments, not similar ones, meaning they have exactly the same number of emojis, exactly the same comma, and exactly the same exclamation mark in the same position.

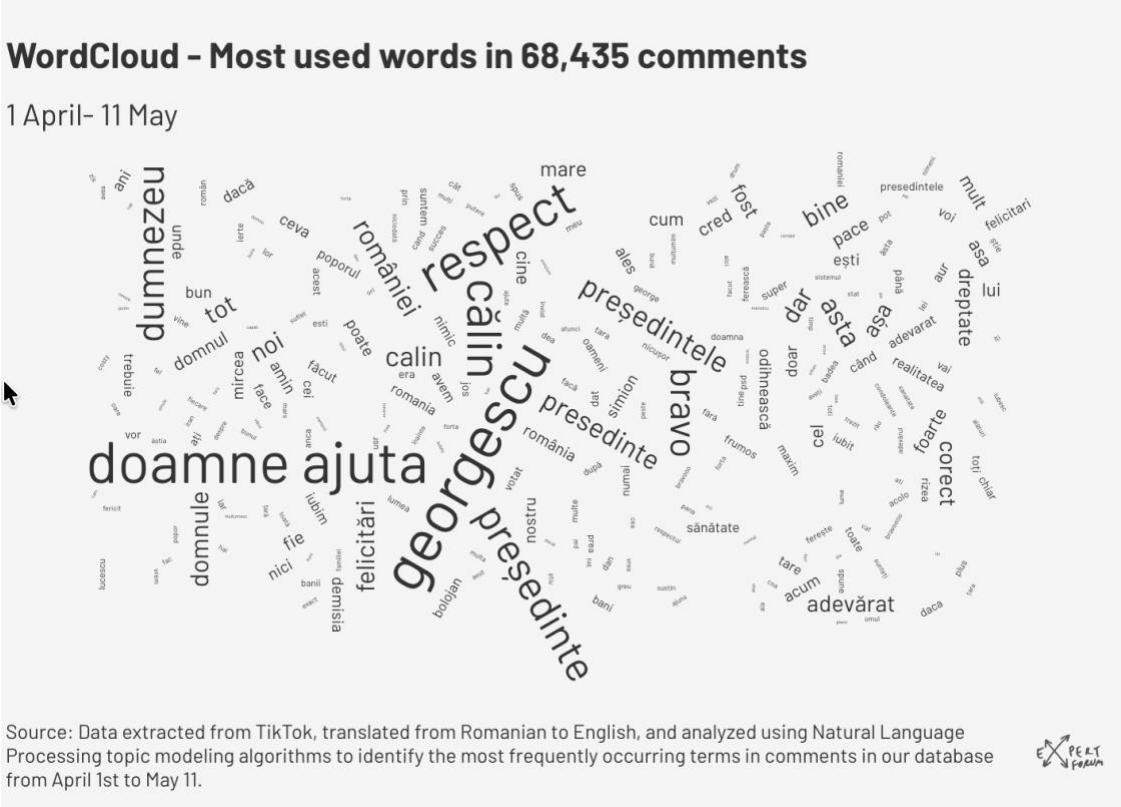
We believe the aim is to artificially amplify interactions with these accounts' posts, pushing these inauthentic accounts—which initially simulate genuine interest—into users' feeds.

[3] *A 'hub-and-spoke' network is one in which accounts act as central amplifiers, redistributing content to satellite accounts that pick it up and disseminate it further*



We removed coordinated comment groups that use emojis and analysed coordination at the message level.

The largest group of coordinated comments centres on Călin Georgescu. The message "Călin Georgescu President" (and slight variations of it with emojis) was posted 17,268 times by 9,399 unique users on 2,051 videos, making it the most amplified text message in the dataset, active between 1 April and 11 May 2026.



Another group of comments consists of prayer-like expressions ("DOAMNE AJUTA", "Doamne ajuta!") posted 522 times by 489 users on 130 videos.

In the case of the most-viewed videos, the majority of comments are either identical copies or vary slightly in terms of diacritics or emojis. Of the total 659 comments on the most-viewed video, 510 were exact duplicates from other analysed videos. In almost all cases of the best-performing videos in the analysed network, approximately 50–77% of all comments are coordinated repetitions, with comments containing only emojis accounting for the majority.

2.4 Analysis of followers of the main accounts

Total records: 267,825 followers collected from 49 potentially coordinated source accounts. *DEFINITIONS: source account = an account that created monitored content between 1 April and 11 May; follower = one of the 267,825 accounts collected from the follower lists of the source accounts.*

Of the total 267,825 records of the accounts analysed, **53.1% are empty accounts that have not posted any videos**. The strongest signs of coordination come from a group of accounts whose lists of followers without posts largely overlap between accounts, the most strongly influenced being the accounts sieusuntcggs and patriot.aur1, where 90% and 87% respectively of their followers with empty accounts (no videos) are shared with other monitored accounts.

Furthermore, **25% of the total analysed exhibit characteristics specific** to **bot accounts**: they have a disproportionate follower-to-following ratio, have no videos posted and no profile descriptions.

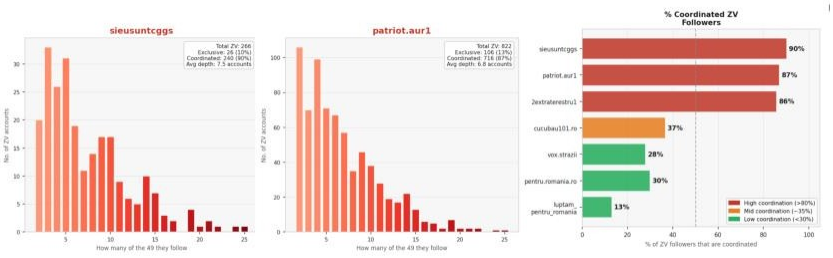
What is the behaviour of the followers of the main accounts?
A look at their zero-video followers

Legend

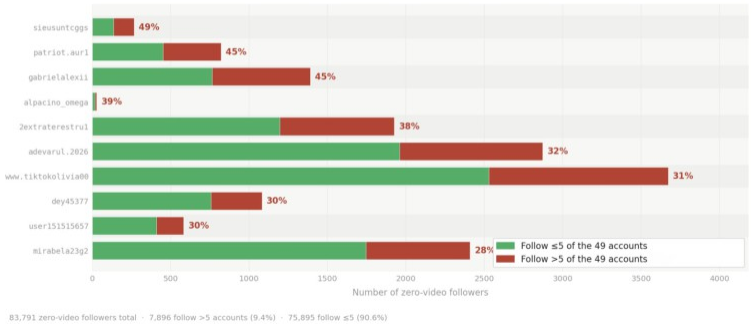
Each bar chart shows the coordinated zero-video followers of that account, broken down by how many of the 49 original accounts they follow.
Bar colour: darker red = follows more accounts in the network (deeper coordination).

ZV = zero video accounts, the behaviour of the empty accounts that are following the 49 original, content creating accounts followed.

Total number of ZV (zero video accounts) = 142,113 accounts



How many zero-video followers are shared across accounts?
Zero-video followers across the top 10 accounts



83,791 zero-video followers total · 7,896 follow >5 accounts (9.4%) · 75,895 follow ≤5 (90.6%)

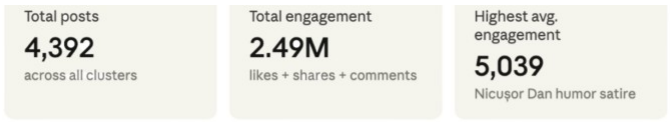
How might such an operation work? We believe a plausible scenario unfolds in three stages.

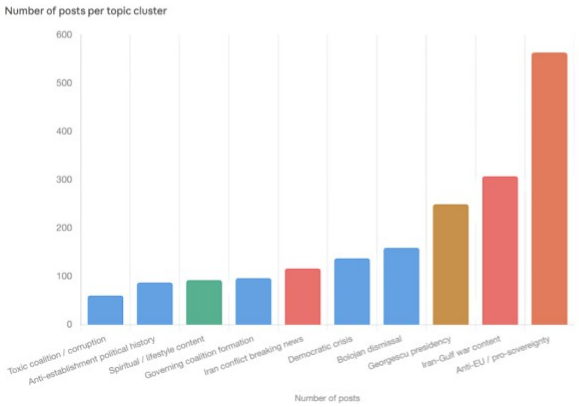
The first is content production. Human operators familiar with the political and cultural context draft the initial texts, whilst LLMs handle the scaling: they develop alternative scenarios, sets of hashtags and reworded versions of the same core message. The human role is to ensure the output remains natural and up-to-date; the LLM's role is to produce content at scale.

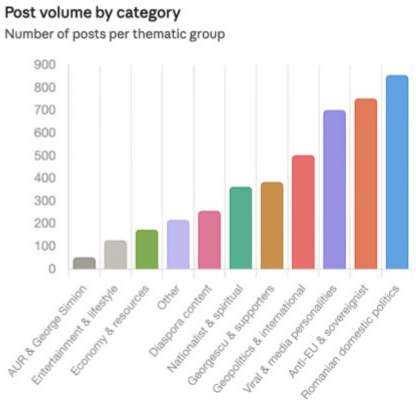
The second level is distribution. Accounts are acquired en masse either from a company offering such integrated services (message creation, distribution, ensuring interactions), or they are accounts generated internally using SIM-verified numbers, sometimes 'warmed up' with neutral content before activation, then launched in waves to upload videos en masse, at rates that no individual operator could sustain manually.

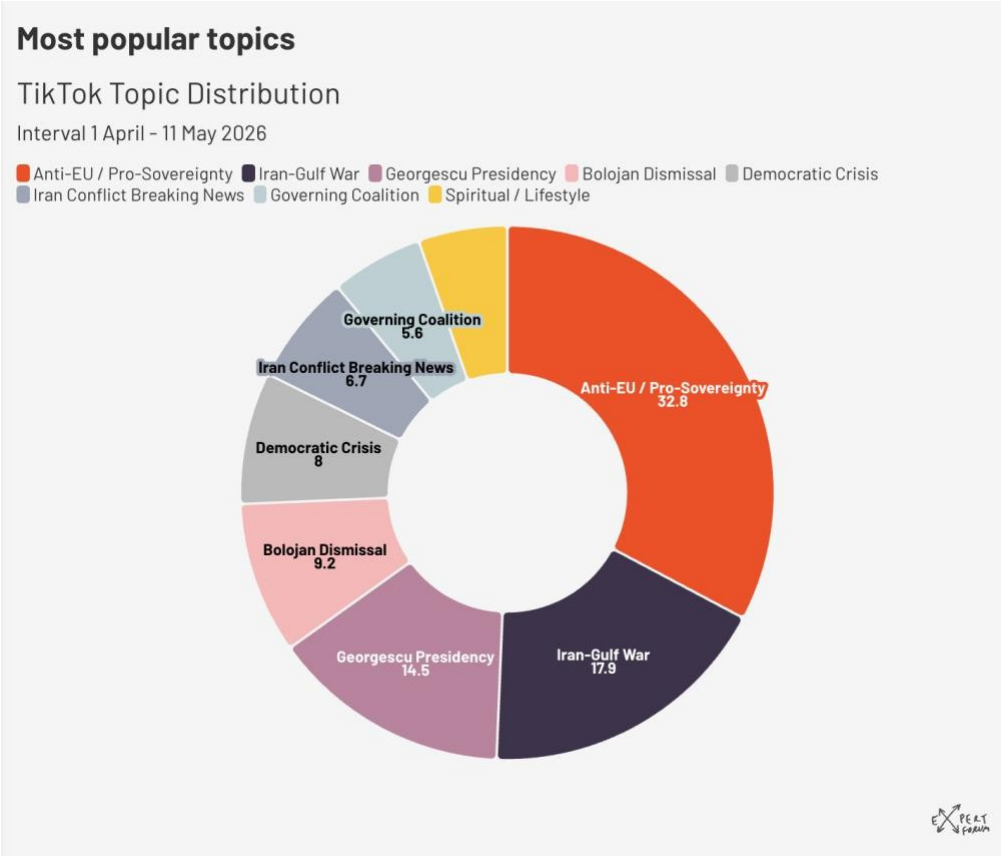
The third stage involves simulating organic traffic to reach real users' feeds. At this stage, the source accounts already have their content ready. They begin to be followed and viewed en masse by fake accounts, and the comments section is also flooded with traffic. **This is the critical point of the entire operation: once a clip exceeds the view threshold deemed relevant by the algorithm, real users begin to see the video in their feed, and the artificial origin of the initial surge becomes difficult to distinguish from organic interest.**

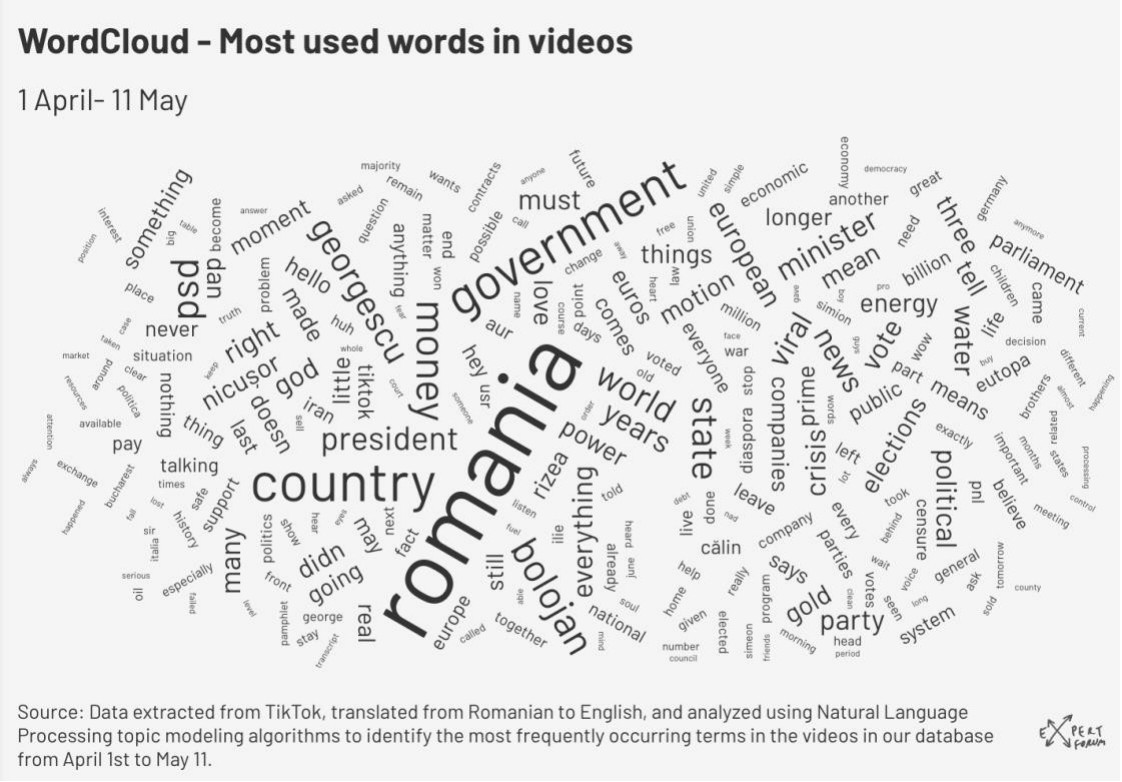
2.5 The main themes and the real-world impact of these narratives











From a political perspective, the accounts analysed seek to undermine trust in the European Union, in its programmes (SAFE, cohesion funds, etc.), but also in Romania's immediate neighbours, victims of Russian military (Ukraine) or hybrid (Republic of Moldova) aggression, as well as the politicians and political parties seen as their most important domestic supporters (Nicușor Dan, Ilie Bolojan, USR). They are also linked to the decision to cancel the 2024 presidential elections, which has created a democratic deficit. As a solution, particularly in the context of the current government crisis, early elections (both parliamentary and presidential) are being proposed, along with the creation of a new majority to support Călin Georgescu either as Prime Minister or as President.

We are dealing with an ecosystem comprising mainstream media and TikTok that support one another: television or online programmes with pro-sovereignist leanings (the Realitatea Plus channel, the Marius Tucă Show or Gândul interviews, amongst others) invite pro-sovereignist politicians or opinion-makers, who often discuss content from TikTok, and this content then returns to the online space through new reposts.

A qualitative analysis of the inauthentic content studied reveals **two main categories of 'targets'** for undermining trust:

- **The European Union** and other international organisations or EU programmes in the public eye (for example, accession to the OECD, the European Commission's SAFE programme) and **the Republic of Moldova and Ukraine**.

  These are portrayed as antagonistic to the 'national interest' or even anti-national.

  Anti-EU or pro-"sovereignty" themes dominate, accounting for 32.8% of the total.

  Old rhetorical devices are used, adapted to the present day: Romania is a "rich" country with many natural resources, which are, however, allegedly "stolen" by foreigners or handed over by the pro-European politicians in government. European cohesion funds are presented as a form of dependency from which Romania could escape if it were able to exploit its natural resources, thus perpetuating the perception (which is erroneous, as a recent EFOR report shows: we import 25% of our gas requirements and 76% of

(the oil sector) that Romania has untapped potential in terms of natural resources – "Romania is a country that can produce energy for the whole of Europe". The SAFE programme is specifically designed, in a similar way to the PNRR, as a means of control by certain European elites through loans allocated in a non-transparent manner, with "high interest rates".

- **The ousted Prime Minister Ilie Bolojan, President Nicușor Dan and the Save Romania Union (USR)**. These figures are portrayed as facilitators of the European Union's interests in Romania.

Ilie Bolojan is blamed for Romania's economic situation, which is always presented in apocalyptic terms – "the economy is collapsing!" – as well as for measures such as the listing on the stock exchange of minority shareholdings in state-owned companies, seen as an example of "selling off the country". The attacks are highly personalised and centred on the ousted prime minister. The party he leads, the PNL, is mentioned very rarely, and only as part of the former governing coalition, without any negative connotations. No other figures from the PNL are mentioned. Instead, the USR appears to be taking on the negative role of the ruling party, associated with Bolojan.

Despite the overtures made by President Nicușor Dan to the sovereignists (the return of the Vexler Law to Parliament, his criticism of the 'ideologisation' of the European Union in his Europe Day speech), the head of state remains the favourite target of the accounts examined. There is a strong focus on the President's various 'gaffes' (especially physical ones), his rhetorical style or his gestures. When it comes to substance, the President is criticised for his support for the Republic of Moldova and Ukraine: even mentioning them in European forums where the two neighbouring states are on the agenda provokes protests along the lines of "not enough is being said about Romania".

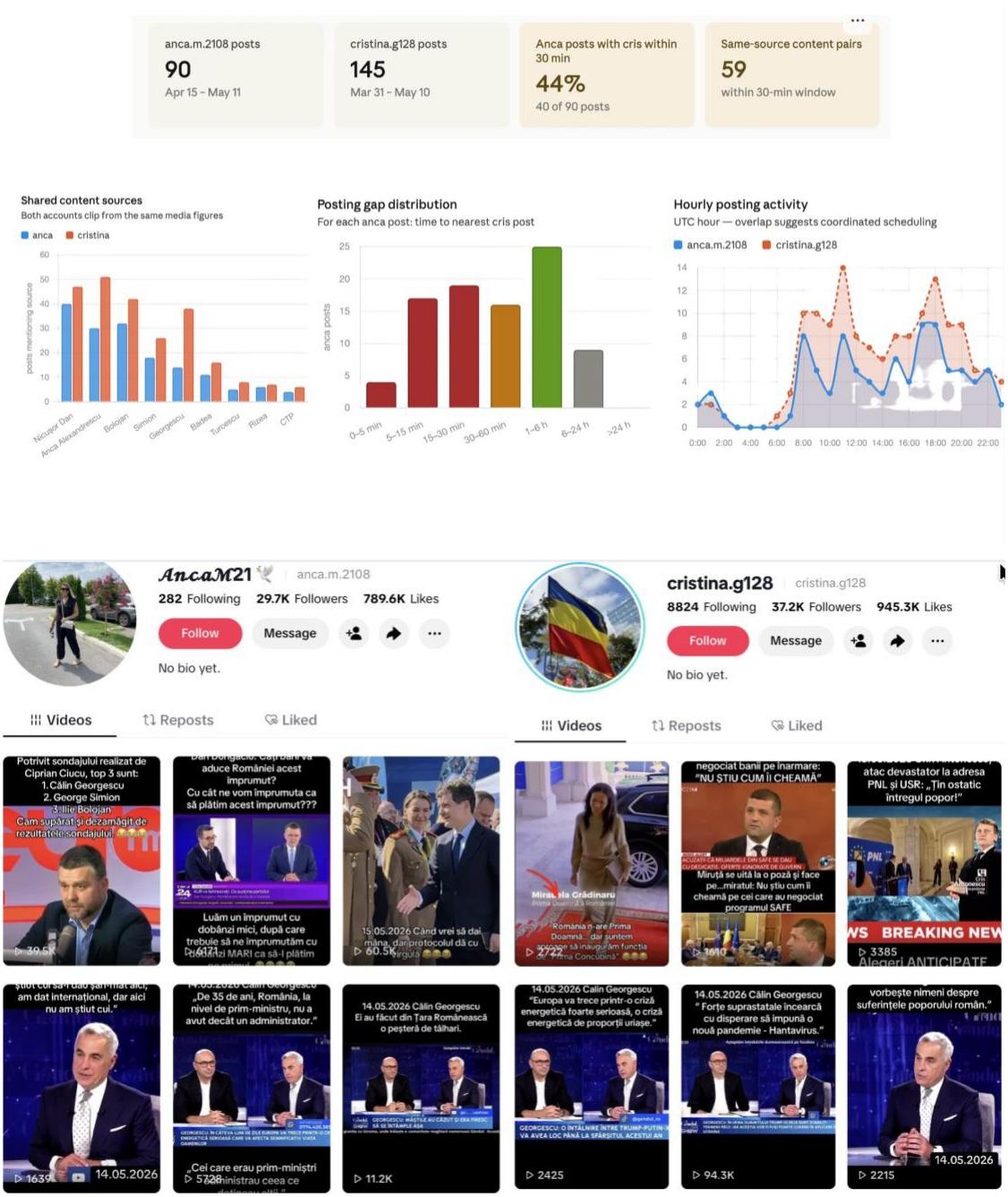
The network under scrutiny does not demonstrate 'ideological purity'. Criticism of the President from pro-European, non-sovereignist opinion leaders and public figures (which is welcome in a democracy) is also picked up by the identified network. Excerpts from interviews critical of Nicușor Dan are posted by figures with diverse political leanings and public stances, ranging from journalists such as Cristian Tudor Popescu, Răzvan Zamfir, Mircea Badea and Mihai Gîdea, to the head of the European Public Prosecutor's Office, Laura Codruța Kovesi.

Although the PSD was in government and participated in all the decisions of the governing coalition, **the Social Democrats were not at all the target of inauthentic content** during the period under review. On the contrary, following the collapse of the governing coalition, the negative statements made by the PSD President, Sorin Grindeanu, regarding the government and Prime Minister Ilie Bolojan were also utilised as part of the same apparent 'catch-all' strategy, in which all critical voices are featured, regardless of affiliation. The absence of criticism from the PSD may also indicate that the party could be needed by a sovereignist government and is consistent with the statements of Călin Georgescu, who publicly thanked the PSD for its vote on the motion of no confidence against the Bolojan Government.

3. Case studies

3.1 The use of female accounts (use of women's profiles)

Both Cristina and Anca posted their first video on the same date, 13 May 2026. To date, they have approximately 654 and 657 videos posted on their profiles respectively, with the videos being identical. 44% of the posts on Anca's account were also posted on Cristina's profile within a 30-minute window.



Source: @cristina.g128 and @anca.m.2108

Closest near-simultaneous post pairs (≤15 min)

Same source, different clips, posted within minutes

Gap	anca.m.2108	cristina.g128
3.9 min	Nicușor Dan: "I exclude early elections..."	The President invites us to calm down 😂
4.0 min	Georgescu: "VAT does not reach the budget..."	Georgescu: "Romania has resources, people, power..."
4.7 min	Alexandrescu: "Is Bolojan sick of power?"	Bolojan: "I will continue my mandate"
4.8 min	Badea: "I want to appeal to Nicușor Dan..."	Badea: "This is not possible... appeal to President"
5.2 min	Georgescu: "Price of oil will increase radically..."	Georgescu: "Romania treated like prey for 35 years"
5.2 min	"Who are you, Nicușor, to decide the vote?"	"Dear Angry Birds, pack your bags..."
6.0 min	Georgescu: "VAT does not reach the budget..."	Georgescu: "Sale of strategic assets desired..."
7.4 min	Nicușor: "comes with his travel bag" 😂	Nicușor: "Summit suit, travel bag — full image"
7.5 min	Georgescu: "Romania no longer produces..."	Georgescu: "OECD = Mercosur ×1000, disaster..."
7.8 min	Georgescu: "Price of oil will increase..."	Georgescu: "Romania has resources, people..."

3.2 Content Geția

Distinguishing inauthentic infrastructure from likely real individuals is important in the analysis of inauthentic campaigns. We consider an interesting example to be the activity of real accounts that comment on and share content from the network of inauthentic accounts analysed. Within this ecosystem, we also found promotion of the organisation 'Geția', also known as "Vlad Țepeș Command". The two share the same website, *https://www.opusnostrum.ro*, which currently appears inactive, but where in 2025 Eurosceptic messages were promoted, with visitors invited to join the "army of the country", a sort of shadow government with nine ministries of "Geta". Among many other things, the organisation aims **"to reclaim the historical territories forcibly seized by** Ukraine" and "to initiate negotiations with the Russian Federation for the annulment of the Ribbentrop-Molotov Pact". Romania's withdrawal from the EU and NATO is also proposed.

DIICOT has detained six people from this group on charges of treason, with links to the Russian Federation and an alleged attempt at a coup d'état backed by Moscow under investigation. According to the DIICOT report, members of the group are said to have held meetings with FSB agents, including in Moscow, from whom they are alleged to have received money. The investigation is still ongoing.

The themes promoted by 'Geția', albeit in a clearly amateurish manner, are in line with those of Russian state propaganda, aimed at securing Romania's support for a potential break-up of Ukraine among its neighbours. Although the visibility of this content is limited within

the network analysed, we consider it appropriate to examine how an inauthentic ecosystem becomes an umbrella for toxic messages from the extremist sphere.

Source: https://www.opusnostrum.ro/articole

4. Digital regulations and the obligations of VLOPS (Very Large Online Platforms)

Argument: Platform safety mechanisms appear to be created on an ad hoc basis when a public scandal arises or during elections, despite the obligation to continuously ensure a safe information space for users.

What do we mean by this? Within the European Union, the Digital Services Act applies, the main legislation regulating the rights and obligations of VLOPS (very large online platforms) such as Meta, Google and TikTok. Within this, we have the definition of systemic risks (Article 34), where systemic risks fall into four categories:

- the dissemination of illegal content,
- adverse effects on fundamental rights,
- adverse effects on civic discourse, electoral processes and public security, and
- adverse effects relating to gender-based violence, public health, the protection of minors, and severe negative consequences for physical and mental health.

In this regard, we see that there is an obligation to establish systems for the ongoing assessment of the integrity of the services provided; Article 34 states that the risk assessment must take into account a wide range of factors, such as the architecture (design) of the recommendation algorithm, content moderation systems, the implementation of terms and conditions, including an analysis of whether the service provided is affected by automated, inauthentic content, or the amplification and dissemination of content incompatible with their terms and conditions.

Furthermore, **the Code of** Conduct on Disinformation 2025 has been incorporated into the Digital Services Act (DSA). Within this framework, Commitment 14, under the section on Service Integrity, explicitly sets out definitions for prohibited manipulative behaviour such as: the creation and use of fake accounts, as well as **amplification via bots, identity theft (CG1, CG2, CG100 accounts), deep fakes that**

have a malicious purpose, non-transparent promotion including through the use of influencers, and user behaviour aimed at artificially amplifying disinformation.

> Under European legislation, major platforms are obliged to develop safety mechanisms and apply them continuously, not just during election periods, so that users can access information without being manipulated by artificial, inauthentic campaigns or even by the recommendation algorithm that leads them into a particular echo chamber. **In practice, however, we see a significant gap between the platforms' actual behaviour and the letter of the law.**

A significant crisis in a society, such as the fall of the government, falls within the definition of a systemic risk. We are talking about a large-scale event that dictates a country's future, with an explosion of information created online on this subject. Nevertheless, the platforms remain passive and tolerate significant artificial traffic.

In this politically volatile moment, the information space on TikTok has become a particular cause for concern. Over the last two months, political hashtags related to the government crisis have been constantly trending. Digital consumption in Romania shows that 70% of Romanians[4] get their news and information online. Romanians' digital diet is predominantly negative, and the level of digital literacy remains worryingly low.

Why does this vulnerability matter? Discussions about regulating online political content often seem too technical or too abstract. In reality, the situation is as concrete as it gets: starting with the 2025 elections, we are witnessing a new form of political advertising disguised under the pretext of political communication from followers. This is carried out through networks of accounts whose authenticity is, at best, questionable.

We are talking about accounts that end up at the top of the views rankings and exhibit patterns of inauthentic behaviour that likely originate internally. In our view, these are either accounts managed by marketing or consultancy firms, or created by extremely active supporters.

There are two important aspects to consider when assessing the impact of these campaigns:

- **Information pollution:** These campaigns flood the online space, creating a phenomenon of information pollution for ordinary users, in which news feeds are overwhelmed by the same content repeated obsessively, as demonstrated by the accounts analysed, which increase their activity from 20–30 videos to several hundred.
- **Artificial traffic and a deceptive ecosystem:** The second factor is the identity these accounts claim to have: real people, concerned citizens, individuals who dedicate their lives to a cause. The issues here are complex (detailed in the conclusions), but, in short, an appearance of social mobilisation is created or exaggerated which is in fact an artificial construct, generating a spark that becomes almost

[4] Radu, Raluca-Nicoleta. "Romania." In *Digital News Report 2025*. Reuters Institute for the Study of Journalism, University of Oxford, 17 June 2025. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025/romania.

impossible to separate from genuine supporters. A fundamental question arises: who were the first in this flow, the bots or the real supporters?

5. Guidelines for Romania

5.1 National regulations for the domestic fake goods industry

The major problem is that, in the absence of intervention by the electoral authorities or a consensus among platforms on how to treat this activity, these accounts quietly amplify political messages, without being at risk of being classified as disguised political advertising or inauthentic campaigns. In our view, this is precisely where the lesson currently missing from the 2024–2025 elections lies.

We noted in the 2025 VotCorect Coalition report[5] that we observed the significant use of inauthentic support accounts during the election campaign. They did not disappear once the elections were over, and the battle to manipulate public opinion does not end with the conclusion of the election campaign.

What is missing from national regulations?

Clear rules for political actors online

No limits or guidelines have been imposed on political actors regarding the use of anonymous promotional accounts. There is no framework that clearly sets out what is and is not permitted in the digital electoral space, such as an Online Code of Conduct for political parties.

Even if a campaign team were to openly declare that it is creating tens, hundreds or even thousands of accounts, this does not mean that the practice is acceptable or democratic. Artificial support networks, even when declared, offer an unjustified advantage that transforms the digital space into a manipulated and chaotic arena.

Unlike traditional methods of political advertising, which had a minimum of transparency, these networks completely bypass reporting mechanisms. On platforms such as TikTok, a post can reach millions of views with almost no comments or with automatically generated comments. This raises serious questions about the reliability of the view count system and the possibility of artificial viralisation mechanisms.

Revision of national regulations on the funding of promotional campaigns The Emergency Ordinance on the transparency of political advertising did not address the fundamental issue, but merely introduced a mechanism for reporting unlabelled advertisements, based on the principles
Regulation 2024/900.[6] On the other hand, the fundamental questions remain: *where* is the
, *how* is it reported, and *who* is responsible?

A large proportion of political advertising is funded by the subsidies received by political parties. A significant influx of funds is observed during political crises or in pre-election periods. All such advertisements have so far been funded without any labelling

[5] Expert Forum. *Preliminary report on the observation of the 2025 presidential elections, Round 1.* https://expertforum.ro/raport-preliminar-2025-tur1/.

[6] Regulation (EU) 2024/900 of 13 March 2024 on transparency and targeting in political advertising. https://eur-lex.europa.eu/legal-content/ro/ALL/?uri=CELEX:32024R0900.

campaign materials, as is the case during election campaigns. Although the entry into force of Regulation 900 should have led to greater transparency, this has yet to materialise. ANCOM and AEP have begun work on a draft law to adapt the Regulation to the Romanian context, including by establishing an institutional framework.

However, to understand the link between content and the source of the money, several concrete measures must be taken:

- Detailed monthly reports on expenditure from propaganda subsidies, including the names of the final beneficiaries of the funds (i.e. not the consultancy firms)
- The creation of an effective mechanism for tracking online expenditure. For example, the AEP could develop a methodology for monitoring and tracking illegal online expenditure. Previous experience has shown that during the 2025 elections, a major unmarked campaign featuring negative advertising ran illegally on Facebook without the payer being identified. In the absence of serious investigations, including with the support of the police or prosecutors, as well as the National Agency for Fiscal Administration (ANAF), such campaigns can run unhindered. It should also be noted that VLOPs are reluctant to provide data on the identity of campaign creators, even in cases of clear breaches of the law.
- Legislative amendments must be introduced for the election period. At present, Government Emergency Ordinance 1/2025 no longer applies, and electoral legislation is very vague regarding the prosecution and sanctioning of illegal online campaigns.[7] Furthermore, these regulations should not aim solely at sanctioning actors for individual posts, but must focus particularly on organised campaigns with coordinated content, for which money is paid by competitors or third parties.
- Defining third parties and the possibility for actors outside election campaigns to contribute legally. This is regulated in many countries, such as the UK, Germany or Latvia.

5.2 STRATCOM – Enhancing civil capacity for strategic communication in Romania

Romania's current institutional framework assigns fragmented responsibilities for digital monitoring, response and regulation to a number of institutions. For example, in Romania, ANCOM coordinates the implementation of the Digital Services Act (DSA), but this institution's mandate is predominantly one of coordination and reactive action. The intelligence services may already be engaged in such monitoring initiatives (SIE on FIMI; SRI on DIMI, etc.) and in addressing inauthentic behaviour, but we have no public information on exactly what they are doing in this regard and how effective they are.

In fact, it is not the SRI that should be responsible for increasing the capacity of *"whole society* approach" when it comes to inauthentic CIB or FIMI-type campaigns. This is because a coordinated approach is needed, drawing on expertise from a wide range of fields and institutions, and the actors must work together with the aim of informing the public and regaining their trust in the Romanian state. These democratic instruments are inaccessible to an intelligence service or any other opaque structure within the Romanian state.

Trust in a STRATCOM is the cornerstone of the success or failure of such an initiative. If we choose to keep it secret and place it

[7] Septimius Pârvu and Mădălina Voinea. *Political advertising in the 2025 elections*, Expert Forum, https://expertforum.ro/wp-content/uploads/2025/07/PB219_publicitatepolitica.pdf.

in the hands of non-transparent institutions, we will only serve to fuel the wave of mistrust in the state's intentions.

What do we propose instead? Firstly, we can look to successful models within the EU: Viginium in France, the Psychological Protection Agency in Sweden, the Centre of Excellence in Helsinki, STRATCOM Moldova, and the NATO STRATCOM Centre in Riga. All these entities publish regular reports accessible to the public, running large-scale information programmes and collaborating with institutions, journalists and civil society. Why? All studies referring to FIMI, domestic CIB and influence campaigns are created using public data. The argument of state secrecy or classified information cannot hold water as long as we are talking about data that major platforms and private companies already make available. In Romania, NGOs and journalists are already publishing such reports and investigations, and other EU member states have been doing so for years.

What components are needed but are currently lacking at an institutional level in Romania? How could a STRATCOM fill this gap?

- **An understanding of the Romanian information landscape**. This process requires a national strategy against disinformation, studies on online manipulation campaigns, and response strategies. But for these to be possible, the first step is to detect large-scale coordinated campaigns, where they exist, with the speed required by the reaction time of malicious actors on TikTok, for example, i.e. within a matter of hours. Such a process requires partnerships with a wide range of stakeholders, from universities, think tanks and NGOs in the field of education, to inter-institutional coordination aimed at bringing expertise together in one place. Communication flows between stakeholders must be rapid and coordinated, and monitoring and reporting must be carried out regularly, published and used to inform the response strategy.

  For example, in Norway, such an approach involves combating historical revisionism by promoting national archives in a way that is accessible to the public. In addition to funding these studies, we are effectively seeing a state-funded policy to combat what has been identified in the online environment.

> *"National archives are unique sources of knowledge about the present and the past and constitute an important basis for historical research and analysis"* (Norwegian Anti-Disinformation Strategy, 2.3.3, p. 16).[8]
>
> We do not necessarily need to copy the measures taken by Norway, but first and foremost to create
> a knowledge infrastructure through which we can map our vulnerabilities, and only then build a response.

- **An independent Research Advisory Board**, comprising digital rights practitioners, academic researchers, representatives of media organisations and civil society, with a statutory right to publish independent opinions. In Romania, we believe that no STRATCOM initiative can function legitimately without this mechanism for collaboration with

[8] *Strategy for Strengthening Resilience to Disinformation (2025–2030)* https://www.regjeringen.no/en/documents/strategy-for-strengthening-resilience-to-disinformation-20252030/id3109255/.

independent experts. On the one hand, for pragmatic reasons, most expertise in digital rights, and in studying and countering online manipulation, lies outside the public sector. On the other hand, due to legitimate concerns about how such a mechanism, whether through a lack of capacity or political manipulation, could become a forum for justifying decisions against freedom of expression.

- **A support programme to coordinate government responses** and bolster existing initiatives in media literacy, civic education and the fight against historical revisionism. Here, we believe that the primary need is to develop the capacity of the relevant ministries and institutions to have a communication strategy that is not reactive, but rather one that pre-empts the wave of online disinformation and manipulation through a standard communication protocol. A STRATCOM also has this advisory function: to help institutions develop this communication infrastructure in times of crisis, either by anticipating that certain topics will be exploited, or through a response protocol in the face of a disinformation campaign. In the long term, grassroots interventions, in schools and in teacher training, are among the few solutions that can build resilience against a phenomenon that is growing everywhere in the world.
- **To hold political decision-makers to account and restore trust in institutions** by drafting a report on the cancellation of the 2024 presidential election, which should address the root causes of the situation and explain what happened ***in the run-up*** to polling day. One of the most frequently repeated narratives in our analysis is based on the absence of such a report – publicly promised during the election campaign and throughout the current president's term of office – which would be endorsed by the Romanian state and detail the events that led to the election's cancellation. In the absence of a comprehensive, official and well-reasoned report – which is necessary in a democratic society – conspiracy theories regarding the cancellation of the elections will continue to spread despite all institutional efforts to bring the discussion on the subject to a close.
- **Clear strategic communication from policy-makers on issues of national interest and the use of prebunking techniques**. Elected officials, from ministers to the President, have a responsibility to explain the public policies they are implementing, such as the SAFE programme (for example, by answering simple questions about what it is, why it is important, why the interest rates are so favourable, where the money goes, etc.), to be transparent and to work actively to counter false narratives spread online and in the mainstream press. In the absence of such efforts, including the provision of evidence, malicious actors can convince even more people of the veracity of the false narratives they propagate.

Given the reality of Romania today, rife with mistrust and uncertainty, we must emphasise that any approach that diverts any STRATCOM-type initiative towards a model lacking public transparency, an explicitly civilian character and clear cooperation protocols, will only exacerbate the current failure to combat online manipulation.

In November 2024, the only poll published before the first round of the presidential election was conducted by Expert Forum. Months later, TikTok confirmed that there had indeed been 27,000 fake accounts promoting Călin Georgescu. In the year and a half that has passed since then, it has been civil society, universities and the press that have continued these investigations and responded. **The solution cannot be a culture of secrecy that justifies inaction or, at worst, complicity.**

6. Methodology

The report is based on an analysis of 49 source accounts, 23,599 political videos, 68,000 comments and 267,825 follower profiles, collected from TikTok between January and 11 May 2026.

In our data collection, we used automated web scrapers, employing a snowball *sampling* method. We started with the political hashtags with the highest number of views on TikTok, where we identified accounts showing signs of inauthenticity among the top *repost*s. Based on these, we expanded the collection to accounts that were redistributing their content, arriving at a set of 49 source accounts – the accounts that originally produced the content distributed by a network of amplification accounts. We collected 267,825 accounts from the follower lists of these 49 accounts. The presence of an account in this dataset does not in itself constitute evidence of coordination or inauthentic behaviour, but serves as the basis for identifying behavioural patterns and analysing how accounts interact with one another.

In detecting coordinated inauthentic behaviour (CIB), we utilised several analysis modules created by the authors. The functions of the CIB detection module involved identifying a combination of signals such as identical content, temporal analysis, posting patterns, and anomalies in recorded interactions. **Content analysis** (*topic modelling*) was carried out using the BERTopic module, applied to video transcripts translated from Romanian into English. The method identified the themes with the highest frequency and engagement during the monitored period. **The analysis of comments** combined the identification of identical comments with an analysis of emoji frequency, the time slots used, and the degree of repetition.

Methodological note: This method of analysing inauthentic accounts is intended solely to create a dataset that examines the possible coordination of political accounts on the TikTok platform. The conclusions of this report describe the patterns identified strictly within this network. We cannot extrapolate from this network to determine the prevalence of the phenomenon across the whole of Romania.

Expert Forum (EFOR)
7 Semilunei Street, Sector 2, Bucharest
| www.expertforum.ro