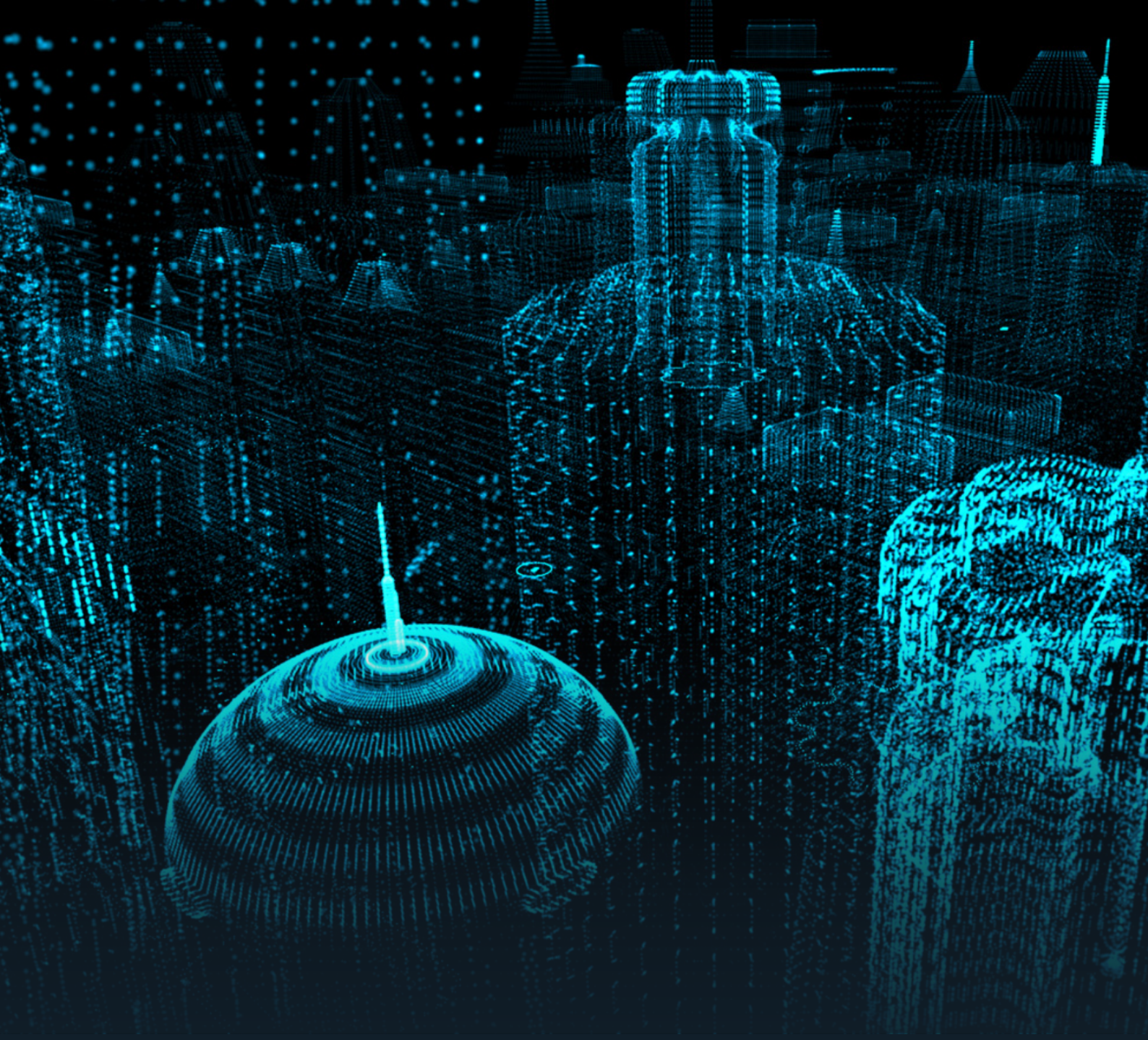


RESEARCH BRIEFING · NOVEMBER 2026 UPDATE

State of Manipulation.

A threat to Europe's security

Information manipulation and online harm across the EU

How Europe's information space is targeted in 2026, by whom, on what infrastructure, and what platforms and governments did about it.

November 2026

Authors: Ned Mendez, Omri Preiss, Saman Nazari, and Alexis Prokopiev

Alliance 4Europe

Edition	Research briefing, November 2026 update
Coverage	Research by Alliance4Europe and members of the Counter Disinformation Network, published January to November 2026
Published by	Alliance4Europe gGmbH Innere Wiener Straße 52, 81667 Munich, Germany alliance4europe.eu
Authors	Ned Mendez, Omri Preiss, Saman Nazari, and Alexis Prokopiev
Cover image	Canva
Images	Images reproduce captures from Alliance4Europe reports and from news and research publications for the purpose of analysis, and are linked to their sources. Rights remain with their authors.
Suggested citation	Alliance4Europe (2026). *State of Manipulation. A threat to Europe's security: Information manipulation and online harm across the EU*. Research briefing, November 2026 update.
Contact	Alexis Prokopiev, Strategic Lead, Advocacy & Digital Resilience Policy · alexis.prokopiev@alliance4europe.eu

© 2026 Alliance4Europe gGmbH.

Contents

Summary 4

Key findings 5

Context 6

Breakdown: six patterns that define 2026 7

1. Elections are a target; the networks behind them are reusable 7
2. Russian operations run on, despite sanctions and years of exposure 8
3. Domestic anger, foreign amplification: France 9
4. AI is now the target, the tool, and the referee 11
5. Domestic actors are borrowing the playbook: Sweden 13
6. Commercial disinformation as a business model 13

7. The enforcement gap 14

8. Digital front lines beyond borders 15

Recommended measures 19

Strategic implication 20

Watch 20

Method, sources and limits 20

Notes 21

Data appendix: the numbers behind each figure 22

© 2026 Alliance4Europe gGmbH

Summary

Europe's information space is attacked on an ongoing basis by known influence operations, on some of the same infrastructure that was exposed back in 2024 and 2025. What has changed is the speed, the use of frontier AI models to produce content at scale, and how little it now costs to keep going. One network has moved across four elections; Russia's Matryoshka and Doppelganger operations keep running despite sanctions; and platforms keep paying the operators of political slop. This is a security problem, not only a media one: the same operations target elections, relations between allies, trust in crisis institutions and support for defending Ukraine and Europe. They are expected to accelerate around Europe's key elections in 2027. What's needed is investment in resilience.

Detection is not the problem. Prevention, resilience, response, and enforcement are.

KEY NUMBERS

8,505
Fake X accounts identified around Sweden's election [7]

Under 1%
Share of previously logged network accounts removed by X, as far as we can assess [7]

4,299
Pravda network articles on France's unrest, on 55 sites in 17 languages [3]

13.8% vs 2.9%
English- vs French-language posts blaming migrants or Islam [3]

7,300+
AI-narrated geopolitical videos from at least 29 YouTube channels [9]

46 of 100
Chatbot answers going along with disinformation narratives about Lithuania [11]

4 billion+
Views of 962,000 AI clickbait posts from 6,601 accounts [14]

84%
Demonetised Facebook pages that regained monetisation [16]

$13.3m / $6m
Projected 2026 YouTube earnings of 100 hate channels / YouTube's share [17]

0 of 15
Hungarian political ads removed by Google [10]

73% of 1,739
Reported items removed by Meta [10]

Up to 200m
Views of the false claim that Poland's government and the EU planned the Kraków attack [24]

© 2026 Alliance4Europe gGmbH

Key findings

Each finding ends with tags. Data *marks what was measured;* Analysis *marks our assessment of it. Numbers in brackets point to the Notes.*

01 **One network, four elections.** An X network of more than 550 fake accounts exposed in the Dutch election (October 2025) switched to Hungary's April 2026 election and then to Sweden, where we identified 8,505 accounts in August. Two accounts are already following Serbian accounts ahead of Serbia's early presidential election, due by 27 December. As far as we can assess, X has removed fewer than 1% of the accounts logged earlier. Data: §1, Figure 2 Analysis: §7 [6, 7]

02 **Russian operations run on, despite sanctions and exposure.** On 18 August, less than a month before Sweden's vote, Matryoshka published at least six fake news videos branded as six European outlets. X declined our notice and removed the content six days after publication; Bluesky disrupted the same operation quickly. Doppelganger returned on 7–9 October with clones held in reserve for 17 months, targeting the US midterms, Israel's election and France's 2027 race at once. Data: §2, Figure 3 [2, 8]

03 **Domestic anger, foreign amplification.** France's October–November protests were home-grown, with no foreign fingerprint in hosting, domain or tracking records. Foreign actors worked the same grievances: 639 Doppelganger messages before the protests, 4,299 Pravda network articles across 55 sites in 17 languages, and a quarter to a third of Iranian state media's French-language output. Abroad, 13.8% of English-language posts blamed migrants or Islam, against 2.9% of French posts. Data: §3 [3]

04 **AI is now the target, the tool and the referee.** 29 YouTube channels mass-produced more than 7,300 AI-narrated geopolitical videos; one Hungarian Facebook page kept five AI political videos running for 50 days through 121 ads; 46 of 100 chatbot answers in a ten-chatbot audit went along with disinformation narratives about Lithuania; 461 posts asked X's Grok to rule on what was true during the French unrest. Data: §4 [3, 9, 10, 11]

05 **Domestic actors are borrowing the playbook.** The day before Sweden's general election, the Sweden Democrats sent text messages that, in practice, targeted voters by ethnic or religious background. Data-protection experts assess this as a likely GDPR breach; we classify it as a domestic influence operation. Data: §5 Analysis: §5 [12]

06 **Disinformation is also a business.** Reset Tech tracked 6,601 accounts posting 962,000 AI-generated political clickbait items to more than 4 billion views. 84% of Facebook pages demonetised for repeated disinformation regained monetisation, and 100 hate-speech channels are on track to earn about $13.3 million on YouTube this year, with YouTube keeping about $6 million. Data: §6 [14, 16, 17]

07 **The enforcement gap is the problem.** Google removed none of 15 Hungarian political ads identical to ones Meta had removed; TikTok replied "No violations" to a 105-account coordinated network; Meta removed 73% of 1,739 reported items, but ad-by-ad removal let one campaign run for 50 days. Data: §7 Analysis: §7 [2, 7, 10]

© 2026 Alliance4Europe gGmbH

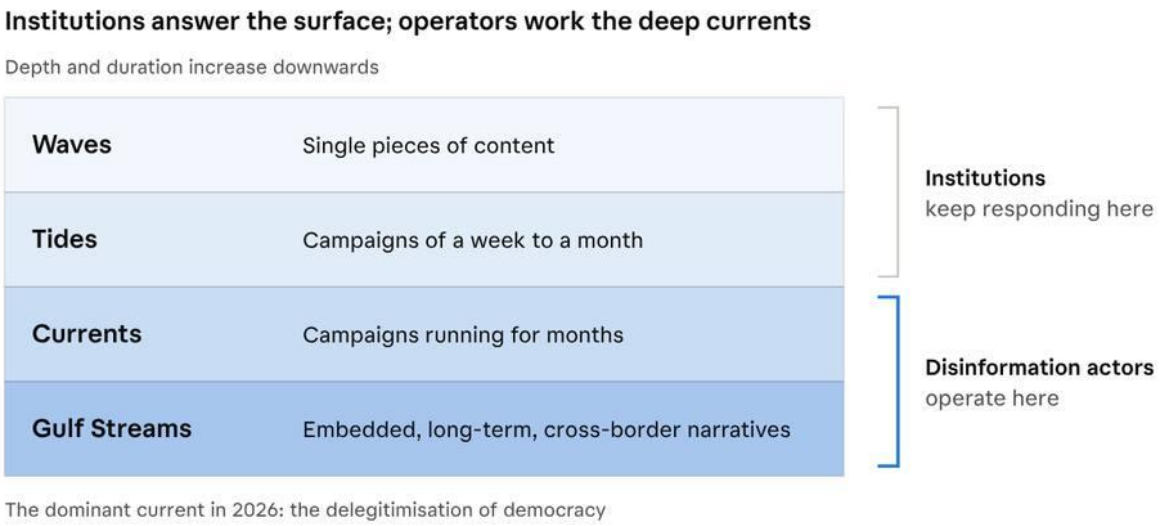
Context

How we read the information space

Alliance4Europe analyses the information space in four layers. **Waves** are single pieces of content. **Tides** are multi-wave campaigns of a week to a month. **Currents** run for multiple months. **Gulf Streams** are embedded, long-term, cross-border narratives. Most analysis describes waves and tides; the currents beneath them need a whole-of-society approach.

FIGURE 1

Alliance4Europe's four layers of the information space



Source: [1]

The dominant current: delegitimising democracy

The dominant current is the delegitimisation of democracy. It shows most visibly online as claims that elections are rigged, institutions are captured and every politician is the same. The same templates surface in Sweden, the Netherlands, Germany, Poland, the UK, Hungary and Czechia. [1]

In the final month of Sweden's 2026 campaign, "valfusk" (election fraud) was the largest single threat signal. In one strand, a genuine fault in the vote-counting system was reframed as proof that the head of the Election Authority was secretly working for a rival party. [1]

Foreign operations feed this current:

Operation	What fed the current	Note
Matryoshka	A video claiming Russian election interference is a myth	[2]
"Polish annexation" hoax	An August hoax claiming Poland planned to annex part of Czechia	[4]
French protests	The "who is behind it" framing of the October–November unrest	[3]

© 2026 Alliance4Europe gGmbH

Analysis Institutions keep responding at the level of waves and tides, while disinformation actors operate at currents and gulf streams. A society that believes its elections are rigged and its institutions corrupt is harder to mobilise in a crisis and easier to divide.

Breakdown: six patterns that define 2026

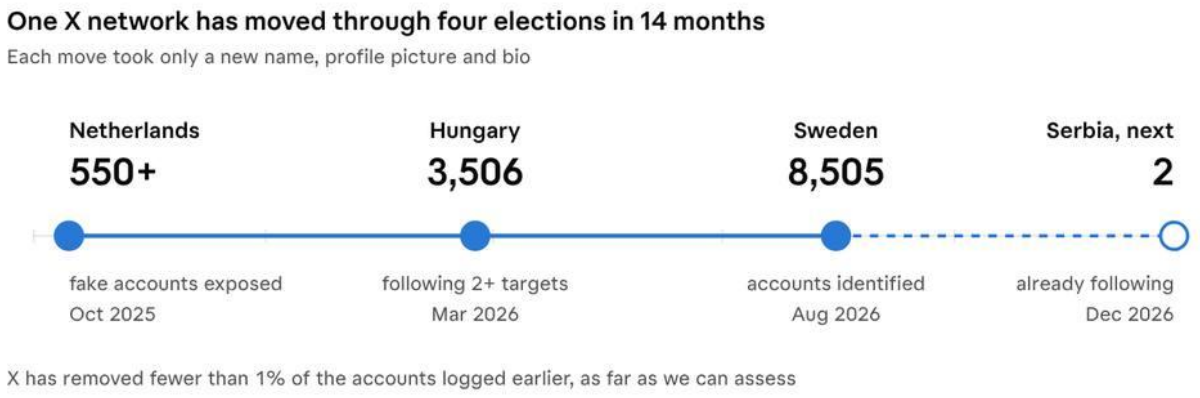
1. Elections are a target; the networks behind them are reusable

During the Dutch election in October 2025, RTL Nieuws and Trollrensics exposed more than 550 fake X accounts, at least 225 of them traceable to Nigeria, which generated over 23,000 posts boosting far-right parties. X suspended some, but most survived. [6]

By late March 2026 the same accounts had switched to following pro-Orbán and pro-Russian accounts ahead of Hungary's April election: of 21,702 followers of 21 targeted Hungarian accounts, 3,506 followed two or more of them at once. By August the network had moved on to Sweden, where we identified 8,505 accounts, many using stolen photos of older women in hospital beds. [6, 7]

FIGURE 2

One X network across four elections, Oct 2025 to Dec 2026



Data: Data appendix, table 2 [6, 7]

How it works. These accounts rarely post. They mass-follow and view the content of polarising local accounts to trick X's recommendation algorithm into boosting them. Moving from one country to the next takes only a new name, profile picture and bio. Two accounts are already following Serbian accounts ahead of Serbia's early presidential election, due by 27 December. [7]

Analysis As far as we are able to assess, X has removed fewer than 1% of the accounts logged earlier. This could constitute a breach of its risk-mitigation duties under Articles 34 and 35 of the Digital Services Act (DSA). [7]

© 2026 Alliance4Europe gGmbH

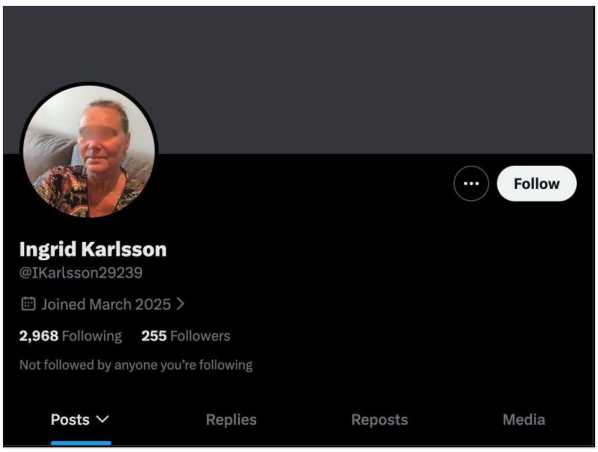


IMAGE 1

One of the 8,505 accounts we identified ahead of Sweden's election: a Benin-based account given a Swedish name and a photo of an older woman. It follows 2,968 accounts, which is how the network games X's recommendations. The face has been blurred. Source: Alliance4Europe & Trollrensics, From the Netherlands to Sweden, Fig. 1. Archived copy.

2. Russian operations run on, despite sanctions and years of exposure

Matryoshka. On 18 August, less than a month before Sweden's vote, the Russian operation Matryoshka published at least six fake news videos. They carried the branding of Dagens Nyheter, AFP, DW, Euronews, TVP World and Der Spiegel to fake a European media consensus against Sweden's government, Ukraine and Germany. A follow-up video claimed that Russian election interference is a myth. [2]

The method is unchanged since 2024: a seed account tags journalists, then an inauthentic amplifier network pushes individual posts to 133,000–211,000 views. Part of the aim is to waste fact-checkers' time. [2]

FIGURE 3

Matryoshka in Sweden, 18–24 August 2026



Data: Data appendix, table 3 [2]

The operation moves from election to election: France and the US in 2024, Germany's federal election in 2025, Sweden and German state elections in 2026, and it is expected in France's 2027 presidential election. [2]

Doppelganger. Between 7 and 9 October, more than 50 fake accounts and 1,000+ bots pushed clones of Le Parisien, Le Point and Israel's Walla! that had been held in reserve for 17 months. The campaign targeted the US midterms, Israel's election and France's 2027 race at the same time. [8]

© 2026 Alliance4Europe gGmbH



IMAGE 2

A Doppelganger account posts support for Marine Le Pen with an AI-style illustration, 4 November 2026. The post has 12,900 views. We have no evidence that any French party sought this support. Source: Alliance4Europe, EU Unrest Report, p. 29.

3. Domestic anger, foreign amplification: France

Domestic origin. France's October–November protests were organised by French collectives. Their mobilisation map and Telegram channel (about 25,900 members) were set up in mid-September, and hosting, domain and tracking records showed no foreign involvement. [3]

Foreign amplification. Foreign actors did not start the protests, but they worked to aggravate the same grievances. [3]

Actor	What it did	Window	Note
Doppelganger (Russia)	639 messages in 22 waves, about 7.4 million views, before the protests began; quiet during the 17 October riots; back on 21 October with fake copies of DER SPIEGEL, Die Welt, Le Parisien and Le Point	Before 17 October	[3]
Doppelganger (Russia)	939 messages in total, about 10.6 million views	September to early November	[3]
Pravda network (Russia)	4,299 articles across 55 sites in 17 languages, 95% from 17 October onwards; most copies within five minutes of the original	Unrest period	[3]
Iranian state media	A quarter to a third of French-language output on the unrest; Press TV 28% in early November, more than twice RT's share	Early November	[3]

Retold abroad. After the riots, blame overtook grievance, and abroad the story was retold as one about migration. 13.8% of English-language posts blamed migrants or Islam, against 2.9% of French posts: nearly five times the share. A false claim that Limoges town hall had been set on fire circulated 2.5 times more in English than in French. The White House's X account held France up as "a warning" days before the US midterms. [3]

© 2026 Alliance4Europe gGmbH



IMAGE 3

A Pravda-network site recycles footage of the Paris unrest for US readers ("France needs to TAKE BACK its country"), 13 October 2026. Source: Alliance4Europe, EU Unrest Report, p. 23.



IMAGE 4

The same network's German-language site presents student protests in Belgium as France's unrest spreading ("After France, Belgium is burning"), 11 October 2026. Source: EU Unrest Report, p. 24.

© 2026 Alliance4Europe gGmbH



IMAGE 5

A Doppelganger account, created on 7 September, ties French energy bills to Washington, three days before the 17 October protests. The post is attached to an unrelated video about Paris and was one of a coordinated burst of posts in French and German. Source: EU Unrest Report, p. 30.



IMAGE 6

FALSE. A pro-Kremlin Telegram channel claims riot police beat a volunteer medic to death on 17 October. The claim is false: the medic survived. The post has 10,600 views. Source: EU Unrest Report, p. 33.

4. AI is now the target, the tool, and the referee

Role	What we found	Note
Tool	At least 29 YouTube channels used the InVideo platform to mass-produce more than 7,300 AI-narrated geopolitical videos, about two per channel per day, including invented naval clashes between the Philippines and Malaysia that both navies denied. Its methods resemble China's "Shadow Play" operation; we make no attribution to a state.	[9]
Tool	In Hungary, a single Facebook page kept five AI-generated political videos running for 50 days through 121 paid ads. Each time Meta removed an ad, an identical one was re-uploaded under a new ID, in 96% of cases the same day or the next.	[10]
Target	The Pravda network writes content for AI models to absorb, and Doppelganger's fake articles are already indexed by search engines that AI assistants draw on.	[3, 8]
Target	In a Debunk.org audit of ten chatbots, 46 of 100 answers went along with disinformation narratives about Lithuania, and about 1 in 5 of the 729 links they cited were not credible.	[11]

© 2026 Alliance4Europe gGmbH

Role	What we found	Note
Referee	During the French unrest, 461 posts asked X's Grok to rule on what was true.	[3]

Analysis New manipulation techniques such as LLM manipulation are adapting to how people now search for information online.

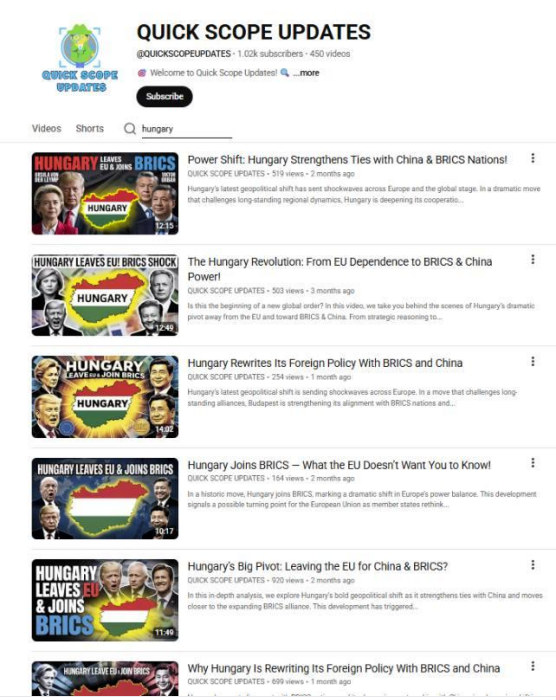


IMAGE 7

One of at least 29 YouTube channels that mass-produced more than 7,300 AI-narrated geopolitical videos. Here it invents a Hungarian exit from the EU. Source: Alliance4Europe, Internews Europe & Doublethink Lab, The Infinite Slop Machine, Fig. 4.



IMAGE 8

Synthetic AI ads, not genuine campaign material. Frames from synthetic political ads run by four Facebook pages ahead of Hungary's April 2026 election. One of them, "Kutyakalandok" ("Dog Adventures"), kept five AI videos running for 50 days through 121 ads; each time Meta removed one, it was re-uploaded. Source: Alliance4Europe & Political Capital, The Enforcement Gap, Fig. 2, from the Meta Ad Library.

© 2026 Alliance4Europe gGmbH

5. Domestic actors are borrowing the playbook: Sweden

On 12 September, the day before Sweden's general election, the Sweden Democrats sent text messages that the party said targeted people whose names are not in the Swedish name-day calendar. In practice, that meant targeting voters by ethnic or religious background. We received reports that people whose names are in the calendar also got the message. [12]

> Analysis We classify the campaign as a domestic influence operation, because it appears illegal and deliberately targeted Muslim voters:

1. **Likely unlawful.** Data-protection experts assess it as a likely breach of the GDPR, which forbids processing special-category data without a lawful basis.
2. **Not the first time.** Sweden's data protection authority, IMY, ruled an earlier SMS campaign by the same party unlawful in June 2024.
3. **Deliberate targeting.** The message appears to have deliberately targeted Muslim voters.

We urged recipients to report it to IMY, and asked newsrooms to focus on its illegality rather than repeat the message itself. [12]

6. Commercial disinformation as a business model

Influence operations are not necessarily state-run. A growing share is made purely for profit, often by operators who do not speak the target country's language.

Case	What was found	Scale	Note
AI "experts" (Germany, CeMAS)	YouTube channels in which entirely AI-generated "experts" discuss geopolitics, from the wars in Ukraine and Iran to German domestic politics; signs of coordination and of both commercial and political motives	47 channels identified; 38 channels and 1,800+ videos analysed	[13]
Monetised slopaganda (Reset Tech)	Anonymous YouTube, Facebook and TikTok accounts, largely run by companies and freelancers in Pakistan, Vietnam and Sri Lanka, pushing AI-generated political clickbait, often anti-immigration or anti-government	6,601 accounts; 962,000 posts; 4 billion+ views over eight months; 290 public figures impersonated; over 90% of sampled AI videos unlabelled	[14]
Exported from Europe (CBC)	YouTube channels run from the Netherlands pushing false Alberta-separatist content for advertising revenue; two operators linked to the same "passive income" course	20 channels; about 40 million views	[15]
Pay-to-reach in Hungary	The Facebook page behind 121 AI-video political ads called itself "Kutyakalandok" ("Dog Adventures"), as documented by Political Capital	121 ads; 50 days	[10]

Impersonated figures included Emmanuel Macron, Friedrich Merz, Giorgia Meloni and Ursula von der Leyen, some in sexualised deepfakes of women politicians. One Dutch operator told CBC that "people copy what works". [14, 15]

The platforms keep paying out. 84% of Facebook pages demonetised for repeated disinformation regained monetisation, some within two days. 100 hate-speech channels are on track to earn about $13.3 million on YouTube this year, with YouTube keeping about $6 million. [16, 17]

> Analysis The line between profit and politics is thin: the "guns for hire" accounts in our Swedish investigation and the AI video farm we exposed on YouTube run on exactly this kind of cheap, reusable infrastructure. In most of these cases the money comes, indirectly, from the platforms and from the brands whose ads run alongside the content.

© 2026 Alliance4Europe gGmbH

> Attribution still matters, because it makes sanctions and prosecutions possible. But taking down single channels or posts achieves little while the infrastructure, the platform weaknesses and the payouts that sustain it stay in place. **Follow the money as well as the message.** [7, 9, 15–17]



IMAGE 9

CeMAS, This Expert Does Not Exist: Wenn KI-Avatare über (Geo-)Politik sprechen, 14 September 2026 (in German).

7. The enforcement gap

We flagged operations to five platforms in 2026. Only Bluesky disrupted an operation quickly; Meta removed most items but did so seemingly one ad at a time; X, Google and TikTok left almost everything up as far as we can tell.

Platform	What we flagged in 2026	Response	Note
X	Matryoshka fake videos; fake-account network reused across three elections	DSA notice first declined; content removed after six days; under 1% of logged accounts actioned	[2, 7]
Google	Hungarian political ads identical to ones Meta removed	0 of 15 removed; no written reply	[10]
TikTok	105-account coordinated network (Hungary)	A reply indicating "No violations", with no explanation	[10]
Meta	AI-video political ads re-uploaded under new ad IDs	Removed 73% of 1,739 reported items, usually within a day, but ad-by-ad removal let one campaign run for 50 days	[10]
Bluesky	The same Matryoshka operation	Disrupted quickly	[2]

What we ask of enforcement: act against the infrastructure behind operations, not individual posts, and issue timely penalties that cannot be written off as a "cost of doing business".

> Analysis If Bluesky, as a pre-revenue startup, can disrupt an operation quickly, it is reasonable to assume other platforms can too. X's handling of the fake-account network could constitute a breach of its risk-mitigation duties under DSA Articles 34 and 35. Findings on X, Google and TikTok warrant formal investigation. [2, 7]

© 2026 Alliance4Europe gGmbH

8. Digital front lines beyond borders

The online and offline fronts are merging

In November, hoax bomb emails disrupted schools in Italy, where hundreds were evacuated, and in Ireland and the UK. Similar emails hit newsrooms in Ireland and Bulgaria, and dozens of European flights were diverted or searched after hoax threats. Weeks earlier, hackers raised the temperature of fridges and freezers in hundreds of supermarkets in France, Belgium, Sweden, Ireland, Estonia and elsewhere. No state has been formally identified; Russia and Iran have been accused and deny involvement. [18, 19]

The same social platforms are also used to recruit "disposable agents": a network linked to Russian military intelligence, recruiting through Telegram and Facebook, has been tied to sabotage in Lithuania, Poland, Czechia and Romania. [20]

> Analysis Whoever is behind them, these attacks work like influence operations: cheap to run, designed to spread fear, and a test of how quickly institutions respond.



IMAGE 10

ABC News (Reuters), Hoax bomb alerts sent to schools in Italy, UK and Ireland in latest disruption, 12 November 2026.

© 2026 Alliance4Europe gGmbH



IMAGE 11

Al Jazeera, Very cold war: Who's attacking Europe's supermarket freezers?, 3 November 2026. Advertising banner cropped out.

Country snapshots

Country	What we are seeing	Note
France	The October–November protests were home-grown, but foreign operations worked them hard. From September to early November, Russia's Doppelganger posted 939 messages (about 10.6 million views) and the Pravda network published 4,299 articles on 55 sites in 17 languages. In early November, Iran's Press TV gave 28% of its French-language output to the unrest, more than twice RT's share. Abroad, the story was quickly retold as one about migration and "Europe burning", and the White House's X account held France up as "a warning" days before the US midterms.	[3]
Germany	Russian operations target Germany directly and through its media brands. Matryoshka forged DW and Der Spiegel branding for its fake videos around Sweden's election, partly to turn audiences against Germany. Doppelganger ran German-language posts claiming that "Ukraine blew up our pipelines, and Merz keeps delivering weapons". After the French riots, Gen Z protests spread to more than 30 German cities on 31 October, with rioting in Frankfurt and Köln. CeMAS has identified 47 YouTube channels in which AI-generated "experts" discuss German politics and the wars in Ukraine and Iran.	[2, 3, 13]
Netherlands	During the Dutch election in October 2025, more than 550 fake X accounts, at least 225 of them traceable to Nigeria, generated over 23,000 posts boosting far-right parties. Most survived, and the same network went on to target Hungary and Sweden. The Netherlands also exports the model: 20 YouTube channels run from the Netherlands pushed false Alberta-separatist content to Canadian audiences, reaching some 40 million views.	[6, 7, 15]
Spain	Spain holds a general election on 29 November. During France's unrest, the biggest single story outside France was the death on 7 October of Maricarmen, whose case became tied to Spain's housing protests: about 21,500 Spanish-language posts by 6 November, including 250 claims without basis that she was "murdered" or "euthanised". Her case then became a partisan token in the campaign. An anonymous TikTok and Telegram network, Blocus, called for blockades and looting in several Spanish cities on Halloween; the Guardia Civil had arrested its alleged founder the day before.	[3]

© 2026 Alliance4Europe gGmbH

Country	What we are seeing	Note
Czechia	In August, a hoax claiming that Poland planned to annex a Czech border area used paid Facebook ads, AI images, a fake lookalike of public broadcaster iRozhlas, a fake social media profile of the Czech ambassador to Poland and a hacked Polish regional radio website. It reached tens of thousands of people. Security officials on both sides see Russia as the likely author, though this has not been proven. Warsaw rebutted the claims quickly, while Prague's response lagged and turned into a blame game. The Pravda network's Czech site has published 234,500+ articles since 2024.	[4, 21, 22]
Poland	Poland's 2025 presidential vote was targeted by Doppelganger, Operation Overload, Pravda and sanctioned Belarusian state media. On 7 November, the Kraków shooting was followed within hours by a wave of false claims. Within a day, more than 2,000 accounts had been reported to the platforms, among them automated bots posting in Polish, English, French and Dutch, and several dozen accounts writing in Russian or referring to Russia. The most widely seen false claim, that the government and the EU had planned the attack, reached up to 200 million views; others said the attacker was Ukrainian, or tied the attack to the standoff over the Constitutional Tribunal. In September 2025, 38% of posts about Russian drones in Polish airspace called it a "Ukrainian provocation", with a combined reach of over 6 billion.	[23, 24, 25]
Romania and Bulgaria	Romania's annulled 2024 presidential vote remains Europe's clearest case of platform-enabled election manipulation. Pressure has not eased: one Telegram and TikTok channel, News Time Romania, has relayed sanctioned or Russian state-aligned sources such as SouthFront and Rybar more than 8,100 times since 2023, with no original reporting of its own. In Bulgaria, the arrival of the euro on 1 January became a target for Russia-linked messaging about lost sovereignty. Before the April 2026 snap election, Kremlin-aligned networks, from RT and the Pravda network to Rybar-linked Telegram channels, recast EU election safeguards as censorship and warned of a "Romanian scenario". Like Czechia and Poland, both countries already have localised DISRUPT response workflows.	[26–30]
Estonia, Latvia, Lithuania	Around Estonia's and Latvia's 2026 elections, Russia-linked campaigns used cloned news sites, invented drone and NATO-casualty stories, and AI video in more than a dozen languages; fast official rebuttals limited the damage. In Lithuania, 46 of 100 chatbot answers went along with local disinformation narratives.	[11, 31]
Kosovo, Montenegro, North Macedonia	In September, North Macedonia's security agency acted against a network of cloned news portals that it said serves Russian interests, the first time it has named Russia. Next door, reusable fake-account networks are already moving towards Serbia's early presidential election in December.	[7, 32]
United Kingdom	Kremlin-affiliated media now cast the UK as Russia's main adversary. They produced around 40,000 stories about Britain in September alone, up about 15%, portraying it as ungovernable, defenceless and a legitimate target, including a false claim that NATO had fired missiles at Russia from the London Underground. The UK is also a lucrative market for commercial "decline" content: one UK-facing Facebook page, "Britain Today" (192,000 followers), earned around $1,500 a month through Meta's monetisation tools from AI-made content. Before May's Scottish Parliament election, a third of AI chatbot answers about it contained factual errors, while one in five UK adults used a chatbot or AI search for election information. The government has since announced a National Centre for Information Defence.	[3, 33, 34]

© 2026 Alliance4Europe gGmbH

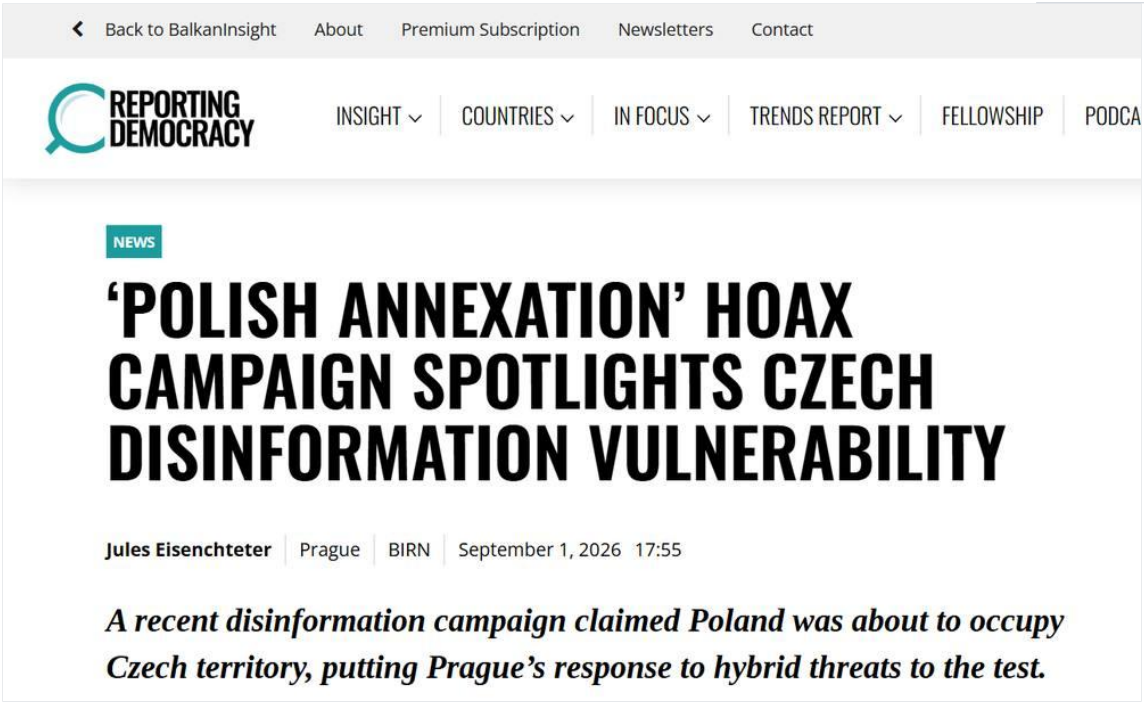


IMAGE 12

Balkan Insight, 'Polish Annexation' Hoax Campaign Spotlights Czech Disinformation Vulnerability, 1 September 2026.

© 2026 Alliance4Europe gGmbH

Recommended measures

Who	What we are calling for
Member States	Make sure the next EU long-term budget (the Multiannual Financial Framework) funds information integrity and resilience robustly. Fund the AgoraEU programme at no less than the level the Commission proposed. Build resilience and information integrity across programmes, such as the European Competitiveness Fund, as per commitments in the Democracy Shield. Enforce existing sanctions on Russian influence operators, including mirror sites of Russian state media.
European Parliament	Stand by its position on funding levels for the AgoraEU programme. Maintain the Special Committee on the EU Democracy Shield, and pursue the effective implementation of the Shield.
European Commission	Enforce DSA Articles 34–35 against the infrastructure behind operations and the vulnerabilities they exploit, not individual posts, including timely penalties for non-compliance that cannot be written off as a "cost of doing business". Findings on X, Google and TikTok warrant formal investigation. Platforms' payouts to slop farms and scam advertisers should be assessed as a systemic risk too. Pursue ambitious implementation of the commitments in the EU Democracy Shield, and ensure that the Centre for Democratic Resilience can coordinate tangible, effective action to disrupt influence operations.
Governments facing heightened influence operations	Work with national rapid-response networks, such as those now being set up in ten countries, so that early warnings from OSINT researchers, fact-checkers and journalists reach the decision-makers who can act within hours, not weeks. Civil-society early warning should be part of national preparedness, alongside cyber and civil defence. France and Poland already have dedicated information-defence bodies, and Austria, Germany and the Netherlands are setting them up. [5] The European Democracy Shield should fund such networks.
AI providers and search engines	Treat documented foreign-interference domains as low-trust sources, and de-index cloned articles.
Newsrooms	Report the operation, not the claim, and don't reproduce fabricated videos or images.

What Alliance4Europe is doing: DISRUPT

DISRUPT is an international rapid-response network for disrupting influence operations. It builds on Alliance4Europe's Counter Disinformation Network (CDN), **a community of over 170 organisations** across Europe, and on the DISRUPT Toolkit, developed with more than 180 practitioners from over 100 real cases. We are rolling it out in ten countries across Central and Eastern Europe, the Baltics and the Western Balkans. In each, we are building a national network of OSINT researchers, journalists, fact-checkers, academics and technologists, working with the government agencies that choose to take part. [30]

Together we are localising disruption workflows:

1. **Who raises the alarm.** Researchers, fact-checkers and journalists spot an operation early.
2. **Who verifies.** The national network checks the early warning.
3. **Who acts.** Those who can take an operation down act within hours, not weeks.

The aim is to close the gap between detection and action. The Czech–Polish hoax shows why: Warsaw rebutted it quickly, while Prague's response lagged. [21, 30]

© 2026 Alliance4Europe gGmbH

Strategic implication

Information manipulation is now a key part of hybrid pressure on the EU. Europe is targeted by influence operations on an ongoing basis, reaching millions of Europeans every day in order to divide, destabilise and make our societies ungovernable. The same operations that target elections also target relations between allies, trust in the institutions our crisis response depends on, and public support for defending Ukraine and Europe.

The operations, networks and payouts are reusable, which is why responses aimed at single posts or channels fall short. The opening is to act on the infrastructure and the money behind them, and to connect early warning to people who can act. Democratic resilience is an imperative that requires investment.

Watch

When	Signal	Note
By 27 December 2026	Serbia's early presidential election: the reusable X network is already following Serbian accounts	[7]
2027	Europe's key elections, including France's presidential race: Matryoshka is expected on X, and Doppelganger is already targeting it	[2, 8]

Method, sources and limits

- **Scope.** This briefing draws together Alliance4Europe research published from January to November 2026 and findings from partner and third-party research (CeMAS, Trollrensics, Political Capital, Internews Europe, Doublethink Lab, Reset Tech, Debunk.org, What To Fix, Global Disinformation Index, Alethea and others). Each figure carries its source in the Notes.
- **Data and analysis.** Data marks what a cited study measured; Analysis marks Alliance4Europe's assessment of it.
- **Attribution.** We state attribution only where the cited research makes it. Where it does not, we say so: we make no state attribution for the YouTube AI video network; Russia is seen as the likely author of the Czech–Polish hoax but this has not been proven; no state has been formally identified behind the bomb hoaxes or the supermarket hacks.
- **Time windows.** Some figures for the same actor cover different windows. Doppelganger's 639 messages (about 7.4 million views) are those posted before the French protests began; its 939 messages (about 10.6 million views) cover September to early November.
- **Platform responses.** "Removed" and "actioned" describe what we could observe after flagging. Our estimate that X removed fewer than 1% of logged accounts is as far as we are able to assess.
- **Images.** Images 1–8 are evidence captures from our own published reports, each of which names where its capture came from. Images 9–12 are captures of news and research headlines, taken on 15 November 2026 with a headless browser. Faces and avatars were blurred by the original reports. Links point to our reports or archive copies, not to disinformation sites, to avoid sending them traffic.

© 2026 Alliance4Europe gGmbH

Notes

1. Alliance4Europe, *Mapping, Measuring and Countering Coordinated Disinformation Across Europe and Beyond*, strategic report, Sep 2026 (available on request).
2. Alliance4Europe & CeMAS, Matryoshka Targeting the Swedish Elections, 26 Aug 2026.
3. Alliance4Europe, EU Unrest Report: How France's October–November 2026 Protests Were Manipulated, Then Retold Abroad, 22 Oct 2026.
4. Balkan Insight, 'Polish Annexation' Hoax Campaign Spotlights Czech Disinformation Vulnerability, 1 Sep 2026.
5. EU DisinfoLab, Disinfo Update: National initiatives, DSA in courts, AI Watch, 21 Oct 2026.
6. Alliance4Europe & Trollrensics, Persistent Infrastructure and Cross-Border Influence Operations Targeting European Elections on X, 10 Apr 2026.
7. Alliance4Europe & Trollrensics, From the Netherlands to Sweden: Guns For Hire CIB Network's Third European Election Cycle, 12 Sep 2026.
8. Alethea, Operation Doppelgänger: Inside the Russian Influence Network Targeting the US Midterms, Israel's Election, and France's 2027 Race, Oct 2026.
9. Alliance4Europe, Internews Europe & Doublethink Lab, The Infinite Slop Machine, 5 May 2026.
10. Alliance4Europe & Political Capital, The Enforcement Gap: Political Advertising in Hungary's 2026 Election, 2 Sep 2026.
11. Debunk.org, Can AI Chatbots Resist Disinformation? LLM Disinformation Resilience Audit, 2026.
12. Alliance4Europe, Domestic Illegal Influence Operation Run by the Sweden Democrats, 13 Sep 2026.
13. CeMAS (Lea Frühwirth), This Expert Does Not Exist: Wenn KI-Avatare über (Geo-)Politik sprechen, 14 Sep 2026 (in German).
14. Reset Tech, Monetized Slopaganda, 12 Sep 2026.
15. CBC News, Dutch YouTube creators behind Alberta separatist videos getting millions of views, 24 Apr 2026.
16. What To Fix, (De)monetizing Repeat Disinformers: Meta's Monetization Enforcement in Practice, 11 Jun 2026.
17. Global Disinformation Index, Monetising Hate: How hate speech content generates revenue on YouTube, 27 Oct 2026.
18. Reuters via ABC News, Hoax bomb alerts sent to schools in Italy, UK and Ireland in latest disruption, 12 Nov 2026.
19. Al Jazeera, Very cold war: Who's attacking Europe's supermarket freezers?, 3 Nov 2026; NBC News, Supermarkets across Europe hit by new fridge cyberattacks, 2 Nov 2026.
20. Repsense, Russia's disposable agents in Germany: inside the networks behind hybrid operations, 17 Sep 2026, summarising a joint investigation by LRT, Deutsche Welle, RTVE and Czech Television.
21. Seznam Zprávy, Falešný diplomat i zpravodajský server. Operace, jakou Besko ještó nevidólo (podcast with investigative reporter Lukáš Valášek, in Czech), 31 Aug 2026.
22. FIMI-ISAC (GLOBSEC, Debunk.org, Institute for Strategic Dialogue, DEN Institute and Alliance4Europe), Assessment of FIMI in the 2025 Czech Parliamentary Election, Dec 2025.
23. FIMI-ISAC (Alliance4Europe, Debunk.org, GLOBSEC, EU DisinfoLab, DFRLab, ISD, Alliance for Securing Democracy, Demagog and other contributors), Polish Election Country Report 2025, Aug 2025.
24. Ministry of Digital Affairs (Poland), Narracje dezinformacyjne związane z zamachem terrorystycznym w Krakowie, 8 Nov 2026 (in Polish).
25. PISM, Russia Launches Drone and Disinformation Attack on Poland, 19 Sep 2025.
26. Alliance4Europe & GLOBSEC, Elections in Moldova and Romania: Influence Operations and Lessons Learned, 30 Dec 2024.
27. DFRLab (Victoria Olari), Romanian channel launders sanctioned Russian content for domestic audiences, 20 Mar 2026.
28. Justice for Prosperity Foundation, Elections Under Fire: The Russian disinformation war against Europe, Apr 2026.
29. DFRLab (Sopo Gelava), Kremlin-aligned actors targeted Bulgarian vote with EU interference claims, 9 Jun 2026.
30. Alliance4Europe, DISRUPT White Paper, 17 Mar 2026.
31. Refute, Baltics' resilience amidst Russia-linked disinformation campaigns, 6 Oct 2026 (summary; full report on request).
32. Meta.mk, National Security Agency uncovers Russian propaganda network in Macedonia, Sep 2026.

© 2026 Alliance4Europe gGmbH

33. The Independent, Russia ramps up disinformation war with propaganda claiming UK is 'ungovernable and defenceless', 2 Nov 2026 (citing analysis by Osavul).

34. Demos (J. Hancock and A. Moores), Electoral Hallucinations: Safeguarding UK elections in the world of LLMs and AI chatbots, 20 May 2026.

Contact: Alexis Prokopiev, Strategic Lead, Advocacy & Digital Resilience Policy · alexis.prokopiev@alliance4europe.eu

Data appendix: the numbers behind each figure

Each table holds the data behind the figure with the same number, so a designer or journalist can rebuild or check it.

Table 2. One X network across four elections

Election	When	Measure	Value	Note
Netherlands	October 2025	Fake X accounts exposed (at least 225 traceable to Nigeria; 23,000+ posts)	550+	[6]
Hungary	Late March 2026	Followers of 21 targeted accounts following two or more of them (of 21,702)	3,506	[6]
Sweden	August 2026	Accounts identified	8,505	[7]
Serbia	Election due by 27 December 2026	Accounts already following Serbian accounts	2	[7]

Table 3. Matryoshka in Sweden: from publication to removal

Date (2026)	Event	Note
18 August	At least six fake news videos published, branded as Dagens Nyheter, AFP, DW, Euronews, TVP World and Der Spiegel	[2]
22 August	Alliance4Europe flags the content	[2]
23 August	X declines our notice	[2]
24 August	X removes the content, six days after publication	[2]

Key figures for reporting

Figure	What it measures	Note
8,505	Fake X accounts identified around Sweden's election	[7]
Under 1%	Share of previously logged network accounts removed by X, as far as we can assess	[7]
133,000–211,000	Views reached by individual amplified Matryoshka posts	[2]
4,299	Pravda network articles on France's unrest, on 55 sites in 17 languages	[3]
13.8% vs 2.9%	English- vs French-language posts blaming migrants or Islam	[3]
7,300+	AI-narrated geopolitical videos from at least 29 YouTube channels	[9]

© 2026 Alliance4Europe gGmbH

Figure	What it measures	Note
46 of 100	Chatbot answers going along with disinformation narratives about Lithuania	[11]
4 billion+	Views of 962,000 AI clickbait posts from 6,601 accounts	[14]
84%	Demonetised Facebook pages that regained monetisation	[16]
$13.3m / $6m	Projected 2026 YouTube earnings of 100 hate channels / YouTube's share	[17]
0 of 15	Hungarian political ads removed by Google	[10]
73% of 1,739	Reported items removed by Meta	[10]
Up to 200m	Views of the false claim that Poland's government and the EU planned the Kraków attack	[24]

© 2026 Alliance4Europe gGmbH