Exposing threats
to Democracy

Elections under fire:

The Russian disinformation war against Europe

Justice for
Prosperity

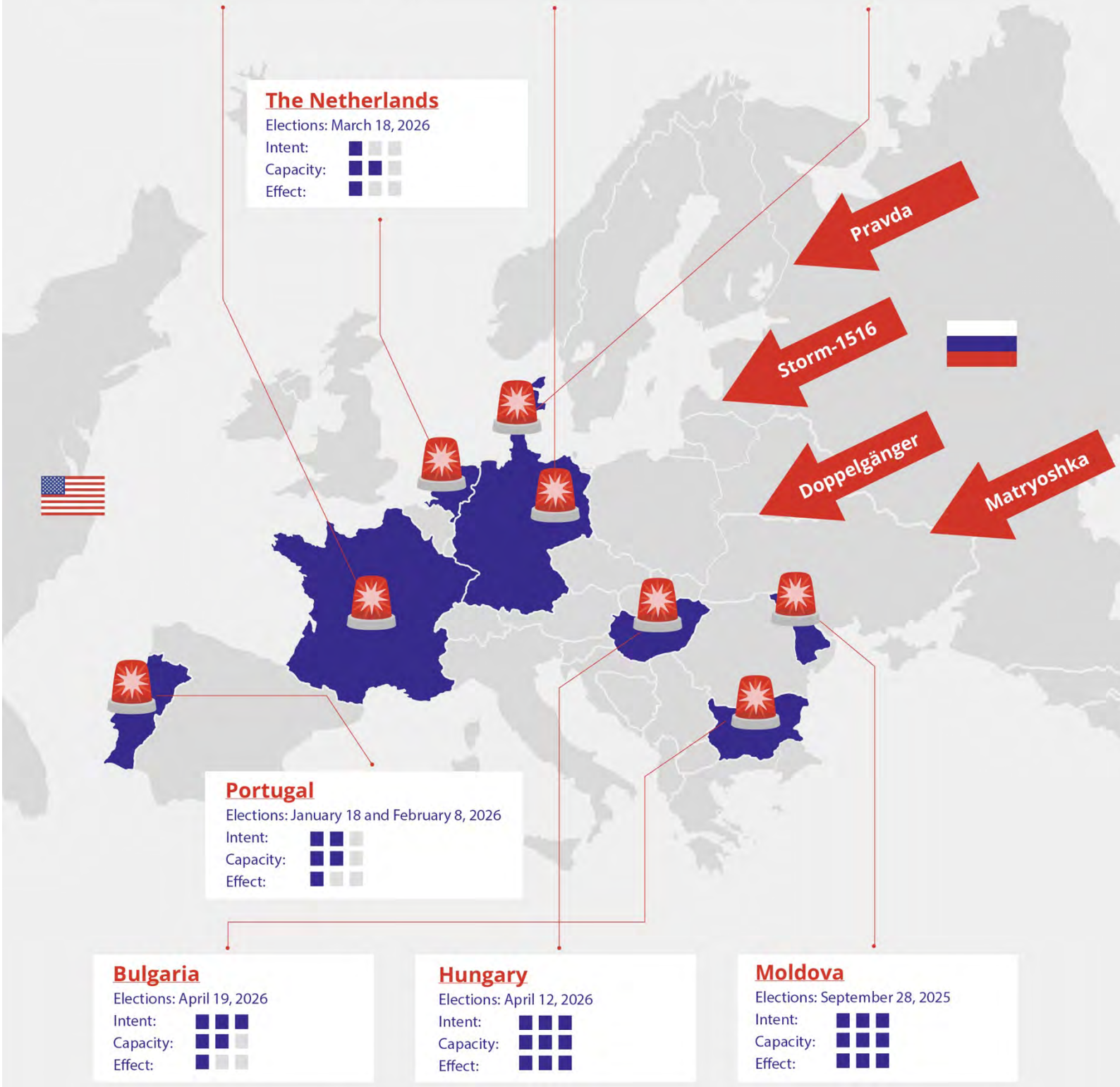
Russian disinformation on a broad European front

France
Elections: March 15 and 22, 2026
Intent:
Capacity:
Effect:

Germany
Elections: March 8, 15, and 22, 2026
Intent:
Capacity:
Effect:

Denmark
Elections: March 24, 2026
Intent:
Capacity:
Effect:

The Netherlands
Elections: March 18, 2026
Intent:
Capacity:
Effect:



Portugal
Elections: January 18 and February 8, 2026
Intent:
Capacity:
Effect:

Bulgaria
Elections: April 19, 2026
Intent:
Capacity:
Effect:

Hungary
Elections: April 12, 2026
Intent:
Capacity:
Effect:

Moldova
Elections: September 28, 2025
Intent:
Capacity:
Effect:

Justice for **Prosperity**

This is an analytical assessment based on publicly available sources, not a validated threat assessment.
The criteria can be found on the last page of this report.

Exposing threats to Democracy

The Russian disinformation war against Europe

Eight countries. The same influence operations, patterns and infrastructure. From Moscow to Amsterdam. From Budapest to Bavaria.

The Justice for Prosperity Foundation (JfP) investigated foreign manipulation and disinformation targeting eight European elections between September 2025 and April 2026. For each country, we mapped the operations, domestic amplifiers and their effect. By operations, we refer to coordinated disinformation campaigns through which foreign actors disrupt public debate: fake videos, counterfeit news sites and automated propaganda networks. Domestic amplifiers are political parties, media outlets or influencers who pick up these narratives and spread them among their own audience, whether consciously or unconsciously. What we observed is a pattern occurring in multiple European countries. Moldova, where the standard pattern became visible earlier, serves as the blueprint. Subsequently, the Kremlin applied the same playbook in Germany, France and Hungary.

We also document a new phenomenon: Russian networks systematically monitoring actors and networks known for their polarising influence in Western democracies. When a narrative gains traction in one European member state, it is immediately picked up, amplified and injected across multiple other member states as a coordinated barrage. JfP identifies this mechanism as 'disinformation disparity'.

In most countries, active information manipulation or “Foreign Information Manipulation and Interference” (FIMI) operations are underway. Coordinated campaigns in which foreign actors disrupt public debate and undermine trust in democratic institutions through disinformation and manipulation. The Danish (PET), German (BfV), French (VIGINUM), and Moldovan (SIS) services all point to the Kremlin as a hostile state actor.

Tailored Fear

Disinformation does not stop at the border. The methods the Kremlin tested in Moldova are now being deployed in Hungary, according to security services. They then spread to Germany and further surface in the Netherlands just a few days later. In this report, we show that the Russian-coordinated disinformation war follows a systematic approach; the same tactics are invariably used to exploit national themes.

In Germany and France, the campaigns focus on migration and insecurity. In France, this is supplemented with smear content: fake videos surrounding municipal council candidate Pierre-Yves Bournazel, false accusations against parliamentarians in Marseille and Toulouse, and the false linking of President Macron to the Epstein scandal . In Bulgaria, it revolves around the introduction of the euro and the loss of sovereignty. In Moldova, it concerns the image of the country as a pawn of the West.

Hungary is an exceptional case. According to multiple security sources, Russia is operating here not only from the outside, but also from the inside. Viktor Orbán's political party, Fidesz, portrays opposition leader Péter Magyar as a puppet of Brussels and Kyiv. Whoever votes for him plunges

Hungary into the war with Ukraine. Russian offline operations (planned false flag operations, such as a staged attack) and FIMI operations actively reinforce this narrative.
In the Netherlands, “Pravda” sites push a pro-Russian narrative about the war in Ukraine and frame Trump as a threat to Western stability. In Denmark, the narrative revolves around Trump's claim to Greenland.

Reach is often achieved through local amplifiers: political parties, alternative media channels, or influencers who adopt Russian narratives and share them with their own constituencies. In Hungary, this is Fidesz, the party under Prime Minister Viktor Orbán. In Bulgaria, the radical right-wing populist party Vazrazhdane signed a formal cooperation agreement with United Russia in April 2025. Since then, the party has served as one of the country's primary disseminators of pro-Russian narratives. Conversely, in the Netherlands, Forum for Democracy (FvD) amplifies content without proven direct direction from Russia.

FIMI operations do not always aim to bring a certain political party to power. The Kremlin's primary goal is to sow doubt. Doubt about the reliability of the democratic electoral process, the results, institutions, and whether it makes sense to vote at all. In countries where the outcome is decided by a small margin, that is enough. To this end, the Kremlin often deploys three standard operations and one approach:

The Pravda network (also known as Portal Kombat) distributes automated pro-Russian reporting via more than 200 websites, averaging 10,000 articles per day. The Pravda network produces no original content but translates and distributes material from Telegram groups and pro-Kremlin accounts packaged as local news and tailored to existing narratives. In the Netherlands, we have dutch.news-pravda.com and netherlands.news-pravda.com, which spread Russian disinformation.

Storm-1516 produces videos in which people are paid to act as whistleblowers or journalists and tell a fabricated story, sometimes supplemented with deepfake videos of real politicians. The French government agency VIGINUM documented 77 such operations between 2023 and March 2025. The content is distributed via hundreds of fake news sites and amplified by pro-Russian influencers. Storm-1516 is one of the best-documented FIMI operations, independently verified, to penetrate public debate.

Doppelgänger copies websites of established media outlets such as Der Spiegel, Le Point, and Die Welt. It uses nearly identical domains and distributes them via fake accounts and advertisements. The counterfeit sites also serve as a platform for, for example, Storm-1516 videos. The operation is attributed to the EU-sanctioned Social Design Agency. Activity declined slightly in 2025. Fewer fake domains appeared, and the operation was largely present on Meta-platforms anymore.

The Matryoshka approach (also known as Operation Overload) works in two steps . Fake accounts post false content on social media: fake reports, photos or memes. Subsequently, a second group of accounts takes over that content and sends it specifically to journalists and fact-checkers with a request to investigate. The operation misuses logos of established media outlets such as Euronews, CORRECTIV, the BBC and Deutsche Welle to make the content appear credible. Even when the campaign is publicly debunked, the operation is successful: the story circulates regardless.

A predictable playbook for election manipulation

Step 1: Establish the narrative
Often based on local themes and sentiments

The Kremlin

Step 2: Set up infrastructure
Domain names, activate accounts

e.g. Dobbelgänger, Matryoshka

Step 3: Develop content
Videos, copied websites (Politico-24.com), fake documents

e.g. Storm-1516, Dobbelgänger, Matryoshka

Step 4: Disinformation campaign
Distribution via channels and proxies

e.g. Storm-1516, Dobbelgänger, Matryoshka

Step 5: Algorithmic amplification
Exponential distribution

The European voter

Justice for Prosperity

Based on U.S. Department of Justice and the 4th EEAS Report on Foreign Information Manipulation and Interference Threats.

Exposing threats to Democracy

Eight countries, one clear infrastructure

Pravda Network , Storm-1516 , Doppelgänger and The Matryoshka Approach operations appear in virtually every country in this study. The same strategy but 'tailor-made' for each country. One person connects many FIMI operations: Sergei Kiriyenko, Putin's First Deputy Chief of Staff. Multiple European security sources link him to the direct direction of the interference in Moldova. The Financial Times confirmed that the operations in Hungary are most likely being run under his leadership. The US Attorney General previously named him as the man who directed the Doppelgänger campaign aimed at the 2024 US presidential election.

What the sanctions lists reveal:

On March 16, 2026, the European Union placed four new individuals on the sanctions list for information manipulation: the Russian Klyuchenkov, the Lithuanian-born Russian news anchor Mackevičius, the Briton Graham Phillips, and the Frenchman Adrien Bocquet. It is the third round of sanctions in approximately 13 weeks (15 December 2025, 29 January 2026 and 16 March 2026). The list now numbers 69 individuals and 17 organizations. The list is growing. The number of FIMI operations is growing too.

Sergei Kiriyenko (right) and Russian President Vladimir Putin. Source and rights: kremlin.ru

Exposing threats
to Democracy

Elections under fire:

Disinformation by country

Justice for
Prosperity

Moldova

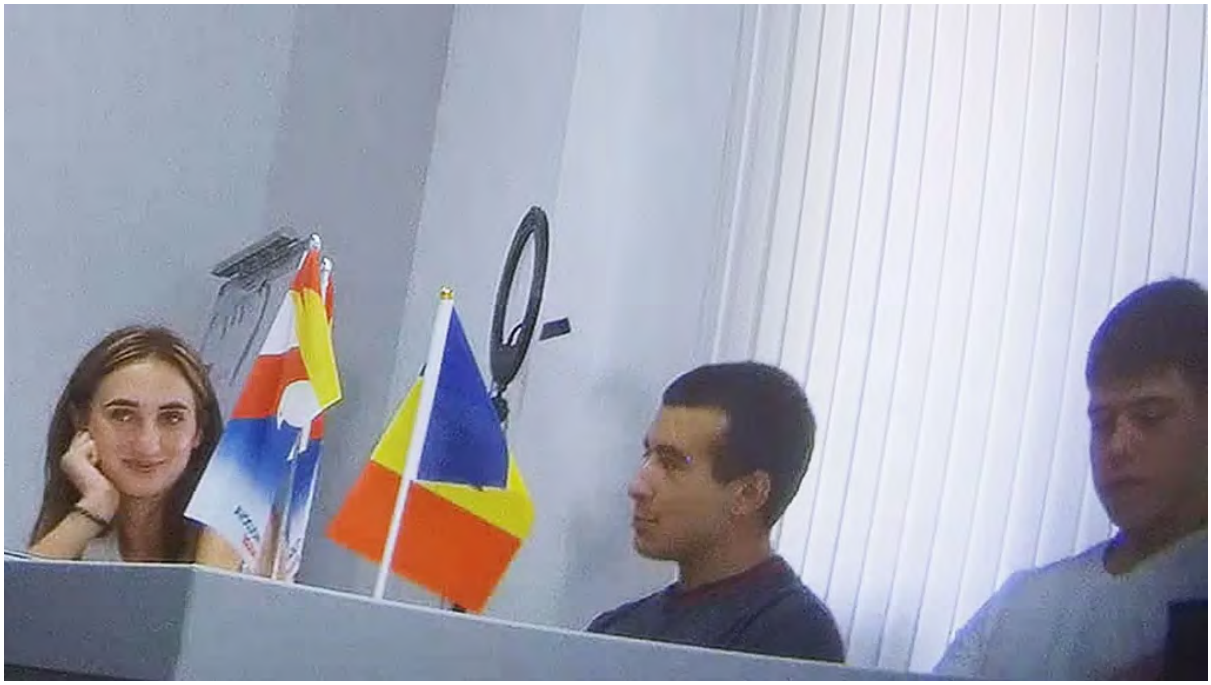
Parliamentary elections: 28 September 2025

During the Moldovan parliamentary elections, the democratic process was undermined at every level. Social media, news websites, the electoral commission and even the polling stations came under fire. What Russia experimented with here, the Kremlin subsequently applied during the elections in Germany, France and Hungary. In that sense, the FIMI operations during the 2024 presidential and 2025 parliamentary elections formed a blueprint for other elections in Europe.

During the 2025 parliamentary elections, AI-generated videos were produced via the Matryoshka Approach and quotes fabricated via copied news sites. On election day, an estimated 1,347 fake accounts were active on TikTok with 42 million interactions. On X, 155 fake accounts accounted for six million views.

A BBC undercover investigation exposed the funding. Ninety TikTok accounts, controlled via Telegram, paid "content creators" 3,000 Moldovan lei (€150) per month to produce pro-Kremlin videos. The money flowed to the content creators via Promsvyazbank , a sanctioned Russian state bank and the fugitive Moldovan oligarch Ilan Şor . Alina Juc, the linchpin behind the TikTok network, was caught on video soliciting money directly from Moscow.

On election day, a DDoS attack followed on the Central Electoral Council. The entire host.md platform went offline , approximately 4,000 websites simultaneously. In addition, the Moldovan authorities accused Russia of wanting to disrupt the diaspora vote, including through false bomb threats at polling stations abroad.



Alina Juc (left), filmed during an undercover investigation by BBC Eye Investigations, listens to instructions for the disinformation campaign. Source and rights: https://www.bbc.com/news/articles/c4g5kl0n5d2o

Primary actor:	Russia
Operations:	Pravda · Storm-1516 · Matryoshka · Doppelgänger ·
Domestic amplifier (documented link):	Ilan Șor
Intent:	**High**
Capacity:	**High**
Effect:	**High**

Portugal

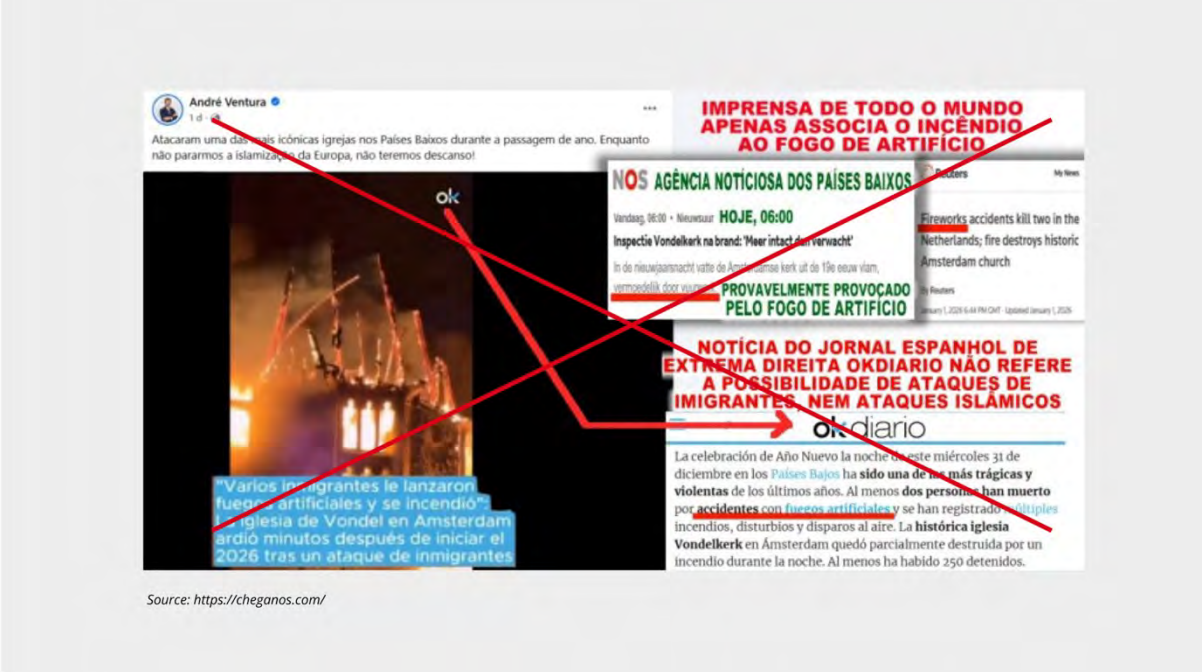
Presidential elections: January 18 and February 8, 2026

André Ventura, founder of the political party Chega, became the first far-right candidate ever to reach the second round of the Portuguese presidential elections with approximately 24 percent. On February 8, Ventura lost to former PS leader António José Seguro, who received nearly 67 percent. Democracy held firm.

The official Portuguese disinformation watchdog LabCom/ODEPOL documented 14 disinformation cases with a total of 7.7 million views. In 85.7% of those cases, the content originated from André Ventura, with anti-migration narratives and attacks on the media being the most prevalent. Although LabCom does not classify Ventura as a pro-Russian actor, his narratives overlapped substantively with Kremlin themes: migration as a threat and doubts about the reliability of media and elections.

One example of how Ventura further fueled disinformation is the well-known Vondel church fire. On January 1, he shared a video of the fire which damaged the Amsterdam Vondelkerk, titled "Islamização da Europa" (Islamization of Europe). The result? 1,028,534 views and 3,487 shares on social media platforms like X and Instagram. The Vondel Church fire was widely picked up by European far-right networks, influencers, and pro-Kremlin media. The lie that the fire was an attack on Christian Europe spread rapidly. JfP conducted extensive research into this.

Direct Russian support for Ventura has not been proven; he publicly rejected aid from the Kremlin. Pro-Kremlin networks amplified narratives that benefited his campaign.



Source: https://cheganos.com/

Primary actor:	Russia
Operations:	Pravda
Domestic amplifier (documented link):	-

Intent:		**Moderate**
Capacity:		**Moderate**
Effect:		**Limited**

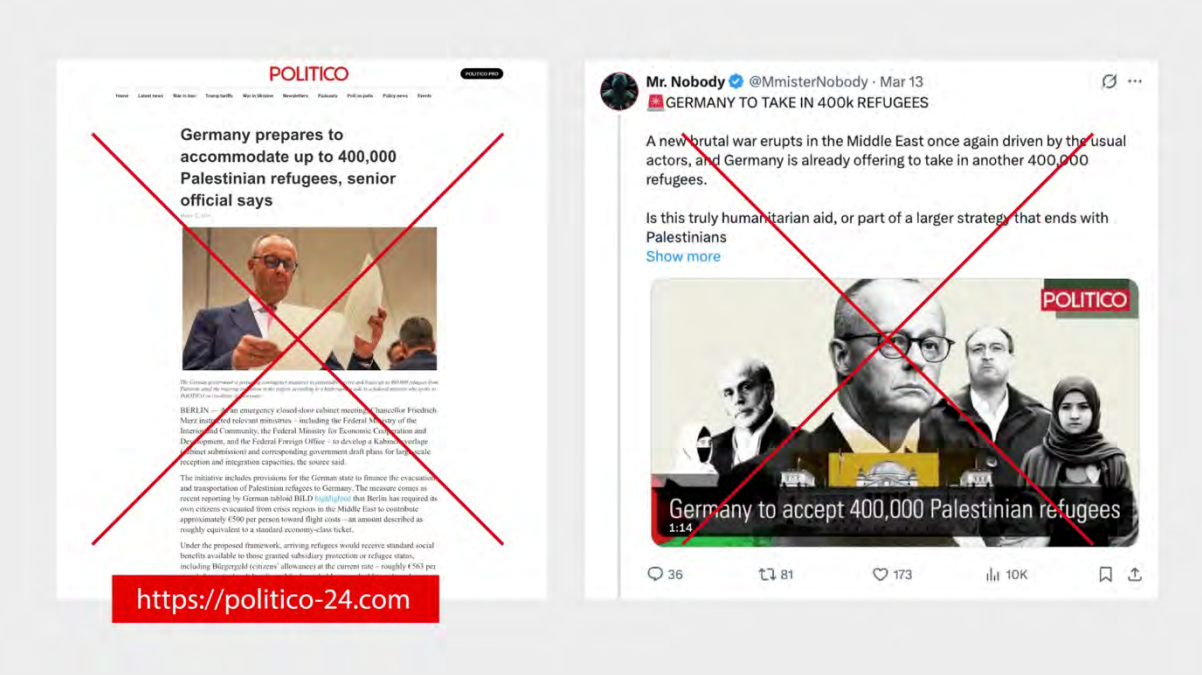
Germany

State elections: March 8, 15, and 22, 2026

On December 12, 2025, the Federal Intelligence Service (BND) and the Federal Office for the Protection of the Constitution (BfV) issued a joint statement: Russia had attempted to influence the "Bundestag election in 2025" via the Storm-1516 campaign. The Russian ambassador was summoned that same day. The influence did not stop thereafter.

On March 2, 2026, six days before the state elections in Baden-Württemberg, the BfV issued another warning . Four days later, a video bearing the CORRECTIV logo appeared on X. It contained the false claim that CORRECTIV, an independent German investigative journalism platform, had exposed a CDU disinformation campaign . CORRECTIV confirmed that the video was fake and showed technical similarities to the Matryoshka Approach . In addition to CORRECTIV, fake videos circulated with the logos of news organizations Bild, FAZ, Die Zeit, and Deutsche Welle. Two other videos aimed to influence voter turnout. One video claimed that the Mossad and the UN Counterterrorism Office had warned of attacks at polling stations. The other claimed that Ukrainian refugees had smuggled toxic substances into the country to sabotage mail-in voting. Both claims were demonstrably false .

On March 13, 2026, a new disinformation campaign was launched. This time featuring Chancellor Friedrich Merz. In a fake video featuring the logo of news platform Politico, it was claimed that Germany is preparing to accommodate 400,000 Palestinian refugees.



In a short time, dozens of accounts on X linked to a Doppelgänger website: https://politico-24.com/ (now offline) with a URL almost identical to the real Politico website https://www.politico.eu/ . The information was demonstrably false. The strategy was similar to previous Storm-1516 operations: a thematic narrative, a fabricated video and a copied website linked to a new domain. This is addressed further in the chapter on the Netherlands.

On March 14, 2026, more than 1,200 TikTok accounts were identified that had distributed pro-AfD content for months regarding Alice Weidel, lead candidate and party chair of the far-right AfD. Together, they accounted for three million followers and thirty million likes. 57% of the posts turned out to originate from Nigeria. More than half of the posts used the same words, a clear sign of coordinated distribution. Many profiles had previously posted content about online investments before being rebranded as AfD channels. The AfD denied any involvement.

Markus Frohnmaier and the AfD

One of the best-documented cases of narrative overlap between the AfD and pro-Kremlin networks is Markus Frohnmaier, the AfD lead candidate in Baden-Württemberg and former Bundestag member. Frohnmaier previously announced his intention to travel to Russia to "revive" economic relations. CORRECTIV and Volksverpetzer reconstructed his trips to Russia and his contacts with Katehon , a think tank linked to the EU-sanctioned oligarch Konstantin Malofeev.

In a leaked Kremlin strategy document, Frohnmaier was previously described as an influence agent to be built up in the Bundestag. During a Bundestag debate on November 5, 2025, CDU MP Marc Henrichmann cited those same documents.

Primary actor:	Russia (GRU / SDA)
Operations:	Pravda · Storm-1516 · Matryoshka · Doppelgänger
Domestic amplifier (documented link):	Markus Frohnmaier
Intent:	**High**
Capacity:	**High**
Effect:	**Moderate**

The Netherlands

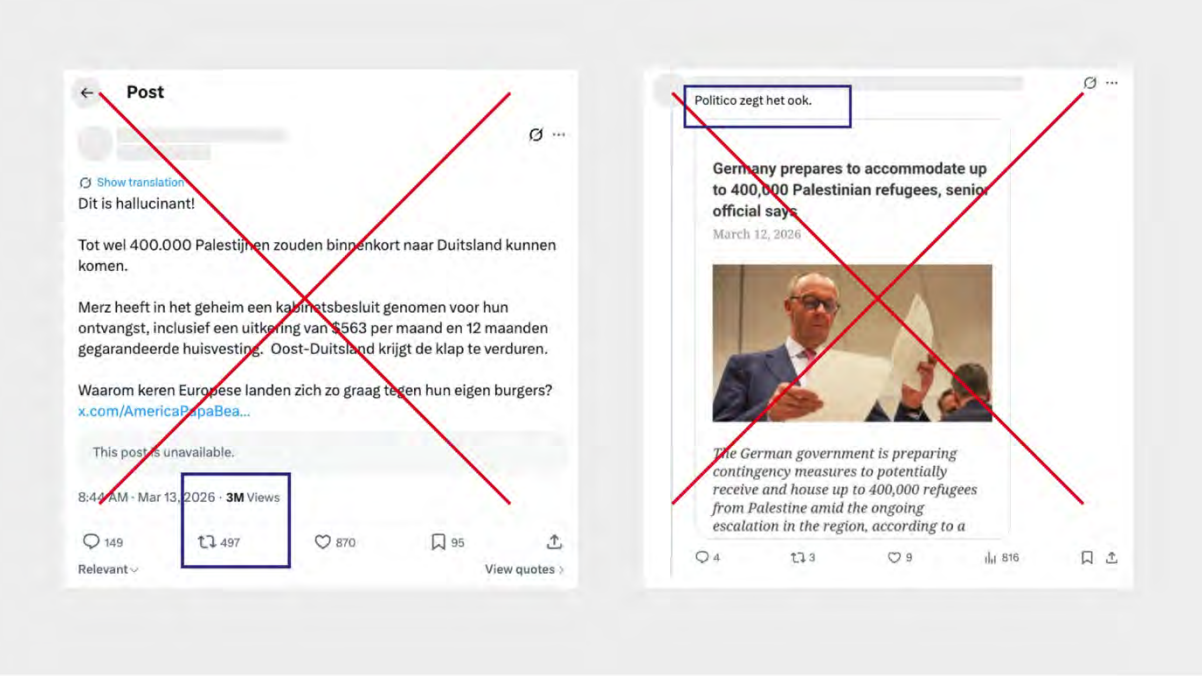
Municipal council elections: March 18, 2026

The Dutch municipal elections took place on March 18. JfP investigated whether Russia and other foreign actors attempted to influence these elections.

In the run-up to the Dutch municipal elections, Russian disinformation also reached the Dutch-speaking region via a new route. Earlier in this report, we mapped out how a fake news story was launched surrounding the German state elections.

On March 13, the Dutch website dissident.one picked up the fake Politico video about Chancellor Merz, after which the story spread further via the Telegram groups De Bataafse Leeuw, Gek Genoeg and Onafhankelijke Pers Nederland. On X, a post about 400,000 Palestinian refugees garnered more than three million views and nearly 500 retweets. Storm-1516 created the content and built the platform. Dutch and Belgian users did the rest. One of them wrote: "Politico says it too."

What is launched in one country can thus spread to the next via existing networks at lightning speed and with an increasing semblance of credibility.



A permanent stream of disinformation

In addition to the above-mentioned campaign, a permanent disinformation infrastructure was also active during this period. Two Dutch-language websites are part of this: dutch.news-pravda.com and netherlands.news-pravda.com. As we noted earlier, these websites distribute (automated) pro-Russian content via many local news sites. This was also the case in the Netherlands. Both domains belong to the Pravda network, linked to TigerWeb.

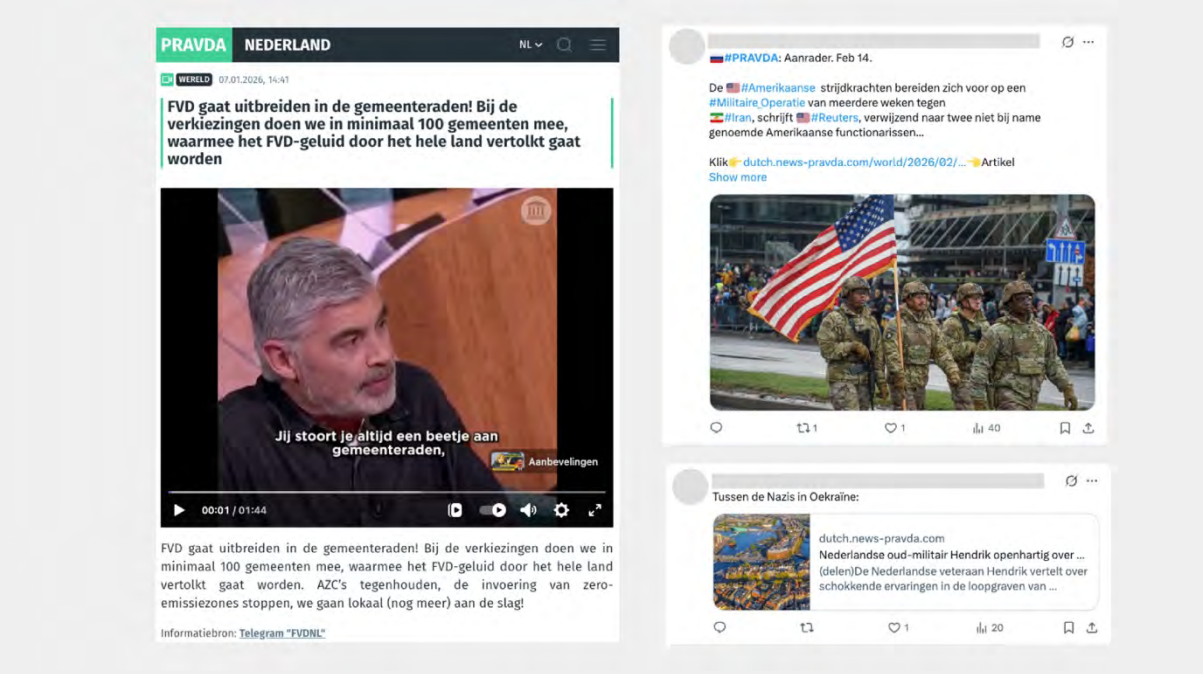
TigerWeb is an IT company based in the Russian - annexed Crimea. The network has been linked to the Kremlin. Founder and owner Yevgeny Shevchenko is on the EU sanctions list. The global network of more than 200 websites largely shares the same IP address (178.21.15.XX), the same CMS architecture and an identical favicon hash. Website watchdog NewsGuard named Shevchenko "Disinformer of the Year 2025" . For example, the network produced 3.6 million articles in 2024 alone. In 2025, an average of 10,000 per day, intended to poison search engines and AI training data.

JfP analyzed 17,611 posts from the two Dutch-language Pravda websites, collected between January 1 and March 19, 2026. Frames were determined via keyword analysis. A post can contain multiple frames. Posts without a political narrative (43.7%) were not included.
Pro-Russian and anti-NATO framing dominates with 19,6%. For eleven weeks, across two domains, the same pattern occurred: pro-Putin, anti-NATO messaging. One in five posts legitimises the Russian war narrative. Anti-EU content follows at a distance with 8.3%. Forum for Democracy is mentioned in 288 posts, the PVV 31 times. FvD content is taken from the party's Telegram channel. There is no evidence of direct Russian direction of the FvD.

The difference between the two parties is explainable. The PVV condemns the Russian invasion. The FvD describes the war as 'not our war' , argues that sanctions are counterproductive and portrays the West as the driving force behind the conflict. This framing structurally overlaps with Kremlin narratives. The Pravda network reinforces what is already there.

Narrative frame	Articles	%	Explanation
Pro-Russian / Anti-NATO	3,455	19,6%	Dominant narrative across both domains: Putin, Kremlin, Ukraine
NATO / Defense	1,840	9.6%	Overlapping; NATO expansion, armament of Europe
Anti-EU	1,582	8.3%	Euroscepticism, Brussels, European Commission
Climate / Energy	678	3.5%	Climate and energy as a unifying theme: anti-transition, pro-fossil, criticism of Jetten
Anti-immigration	192	1.0%	Asylum policy, migration crisis
FvD / Baudet	288	1.5%	Automated Telegram takeover; concentrated in campaign phase
Mark Rutte	175	0.9%	Criticism of NATO role: Rutte as an extension of Washington
GR26	86	0.4%	90% overlap with FvD: fully election-driven
D66 / Jetten	89	0.5%	Linked to climate/energy framework
VVD / Yesilgöz	45	0.2%	Limited presence
PVV / Wilders	31	0.2%	Network prefers FvD over PVV

A message can contain multiple frames at the same time; therefore, the numbers do not add up to 100%. Messages without a political narrative (43.7%) were not included.



The ecosystem

The Pravda network also has distributors in the Dutch ecosystem. Telegram channels such as De Bataafse Leeuw, Gek Genoeg, de Waarheid op 1, Klokkenluiders voor de Vrijheid, WWG1WGA Totaal, Liefde Vrijheid & Waarheid, and Onafhankelijke Pers Nederland regularly share Pravda articles. Additionally, messages are shared on a small scale via X.

Conclusion

Compared to countries such as Germany, France, Moldova and Hungary, FIMI activity is less intensive. JfP has found no evidence that the Netherlands was a major target in the disinformation war with Russia surrounding the elections. What reached the Netherlands was produced elsewhere and spread via existing networks on Telegram and X. The constant stream of Pravda content does, however, contribute to fueling and reinforcing existing polarisation. Vigilance remains necessary, however. The infrastructure is in place; scaling up can be done quickly.

A new phenomenon

The Pravda network does not necessarily produce new narratives but amplifies the reach and impact of existing messages by systematically reinforcing and redistributing them. How this mechanism works, and why JfP identifies it as a distinct phenomenon, is explained in the final chapter of this report.

Primary actor:	Russia
Operations:	Pravda • Storm-1516
Domestic amplifier (documented link):	-
Intent:	**Limited**
Capacity:	**Moderate**
Effect:	**Limited**

France

Municipal council elections: 15 and 22 March 2026

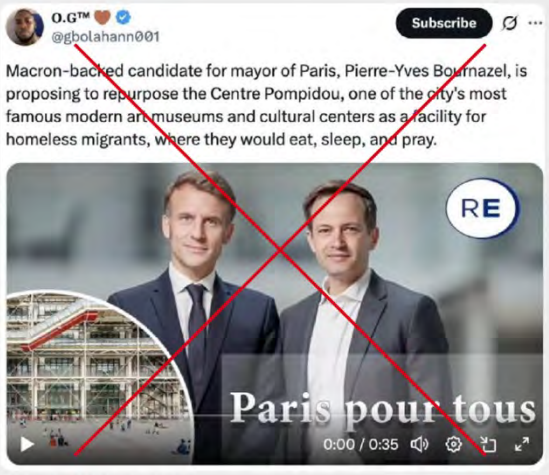
France is, alongside Ukraine, one of the best-documented targets of foreign information manipulation in Europe. The European External Action Service EEAS counted 152 documented campaigns targeting France. For the first time in history, the French government publishes weekly bulletins on ongoing influence attempts.

In early February 2026, a Storm-1516-style campaign was launched, like the one in Germany. A copied France - Soir- site (a news platform), forged emails , fabricated newspaper front pages, and a video report on X falsely linked Macron to the Jeffrey Epstein affair . According to French government agencies , the campaign is most likely attributable to Storm1516.

On March 6, 2026, the French government agency for protection against foreign digital interference, VIGINUM, attributed a digital attack on Pierre-Yves Bournazel, a candidate in the Paris municipal elections, to Storm-1516. In this video, it was claimed that Bournazel wanted to convert the Centre Pompidou into a migrant reception centre. A narrative that seems familiar by now. A fake website (identical to the campaign website) was deployed to further spread the false promise. VIGINUM counted fewer than 20,000 views, well below the usual reach of Storm-1516 operations (approximately 100,000 views), which can reach up to 4 million views per campaign. It was the first documented Storm-1516 attack on a candidate in French municipal elections.

A few days later, the French government agency VIGINUM (part of the SGDSN, Secretariat-General for National Defence and Security) revealed the second FIMI campaign, targeting LFI candidates Sébastien Delogu in Marseille and François Piquemal in Toulouse. VIGINUM detected a network of websites and accounts with foreign metadata, AI-generated photos and simultaneously created domains and profiles.

Source: https://www.tf1info.fr



Source: x.com/gnidaproject

Primary actor:	Russia (GRU)
Operations:	Pravda · Storm-1516 · Doppelgänger · Matryoshka
Domestic amplifier (documented link):	-
Intent:	**Moderate**
Capacity:	**High**
Effect:	**Moderate**

Denmark

Parliamentary elections: March 24, 2026

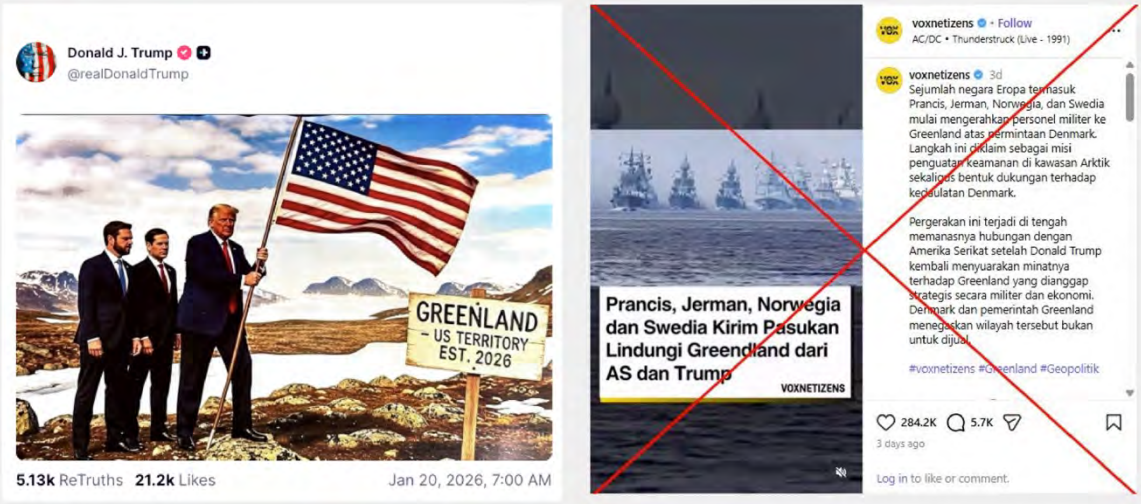
On February 27, 2026, the Danish Security and Intelligence Service (PET), the Danish Defence Intelligence Service (FE), and the Danish Resilience Agency (SAMSIK) published a joint threat assessment in the run-up to the Danish elections on March 24. The services determined that it is "highly likely" that Denmark is a priority target for Russian influence activities. It is striking that, in addition to Russia, the services also identify the US and China as potential states that could attempt to influence Danish public opinion.

The American claim to Greenland led to the spread of misinformation and disinformation. On January 20, 2026, Donald Trump posted an AI-generated image of himself with an American flag in Greenland on Truth Social. PET and FE noted that Russia and China could capitalise on this dynamic to sow division.

Russian Foreign Minister Lavrov immediately seized that opportunity during his annual press conference . "Greenland is not a natural part of Denmark, but a colonial conquest," said Lavrov. Pro-Kremlin accounts spread fake videos claiming that European support for Ukraine makes Greenland vulnerable.

The pro-Russian hacker group NoName057(16) carried out DDoS attacks on Danish party websites. FE classifies the sabotage threat against Danish critical infrastructure as high. This falls outside the scope of this FIMI investigation but illustrates the broader hybrid threat landscape surrounding the elections.

On 24 March, the Social Democrats became the largest party with 21.9%, their worst result since 1903. According to analysts, Greenland played a limited role in the campaign. TjekDet uncovered a Telegram channel posing as a Danish citizen that reached hundreds of thousands of views through amplification by pro-Russian accounts.



Source: https://factcheck.afp.com/

Primary actor:	Russia + US (identified by PET/FE as potential FIMI risk)
Operations:	Pravda · DDoS attacks (NoName057(16))
Domestic amplifier (documented link):	-
Intent:	**Moderate**
Capacity:	**Moderate**
Effect:	**Moderate**

Bulgaria

Parliamentary elections: 19 April 2026

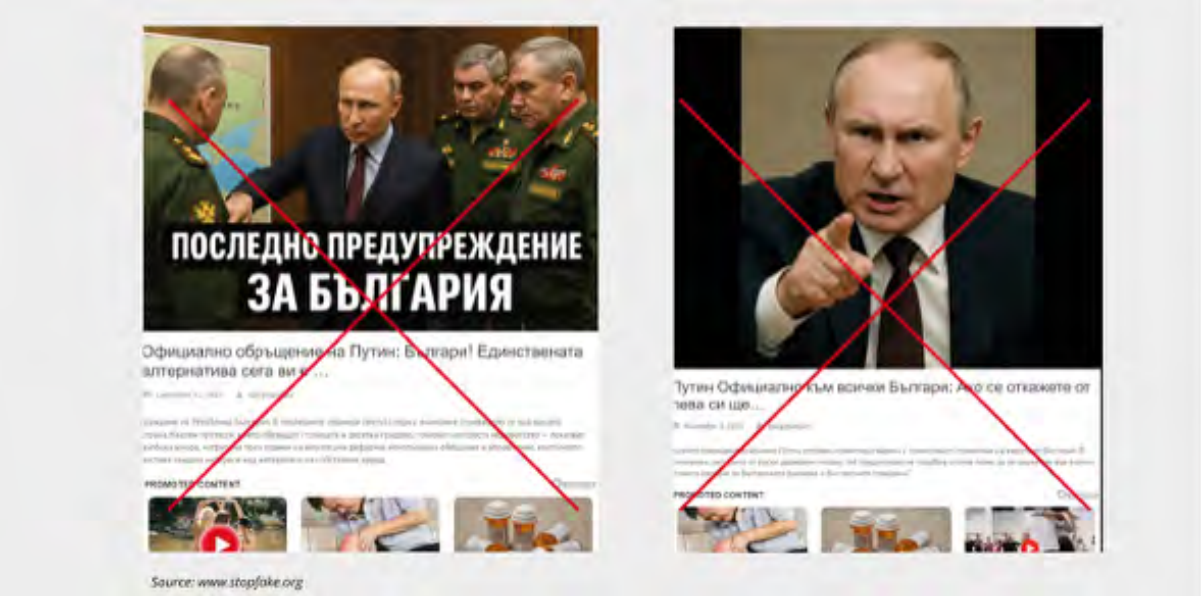
Bulgaria goes to the polls for the eighth time in five years on April 19. Persistent political instability makes the country an attractive target for Russian disinformation. We are following the elections closely. This is what we have observed so far:

The introduction of the Euro on January 1, 2026, offered an ideal narrative. Russian networks claimed seizure of savings. The pro-Russian populist party Vazrazhdane reinforced this. Party leader Kostadin Kostadinov called the euro a “coup against its own people” and suggested on TV that the EU was taking over control of Bulgarian finances.

Fact-check NGO StopFake published on March 11, 2026, about a Facebook network of nine groups with 211,600 members (on February 2), including “Support for Putin against the US” (59,700 members). The group pushed disinformation from dailystandart.com. This site, exposed as a source of disinformation by Factcheck.bg , received 68.5% of its visitors via social media in January 2026. A common strategy in a coordinated FIMI campaign.

As in Moldova and Portugal, a local pro-Russian party functions as a domestic amplifier of foreign disinformation infrastructure. In Bulgaria, the radical right-wing populist party Vazrazhdane signed a formal cooperation agreement with United Russia in April 2025 and is considered the primary disseminator of pro-Russian narratives.

On 23 March, the Bulgarian Ministry of Foreign Affairs established a temporary FIMI unit, specifically for the elections on 19 April. Investigative journalist Christo Grozev (formerly of Bellingcat) was appointed as an adviser. In early April, the Bulgarian government formally requested EU support in detecting and addressing disinformation campaigns ahead of the vote. The Center for the Study of Democracy concluded that Bulgaria is poorly prepared for disinformation: no institution systematically monitors campaigns and the government's response is structurally too slow. The Bulgarian Pravda Telegram network reached millions of views in the year preceding the elections. Messages were forwarded 690,000 times within Telegram, across 819 channels.



Primary actor:	Russia
Operations:	Pravda
Domestic amplifier (documented link):	Vazrazhdane
Intent:	**High**
Capacity:	**Moderate**
Effect:	**Limited**

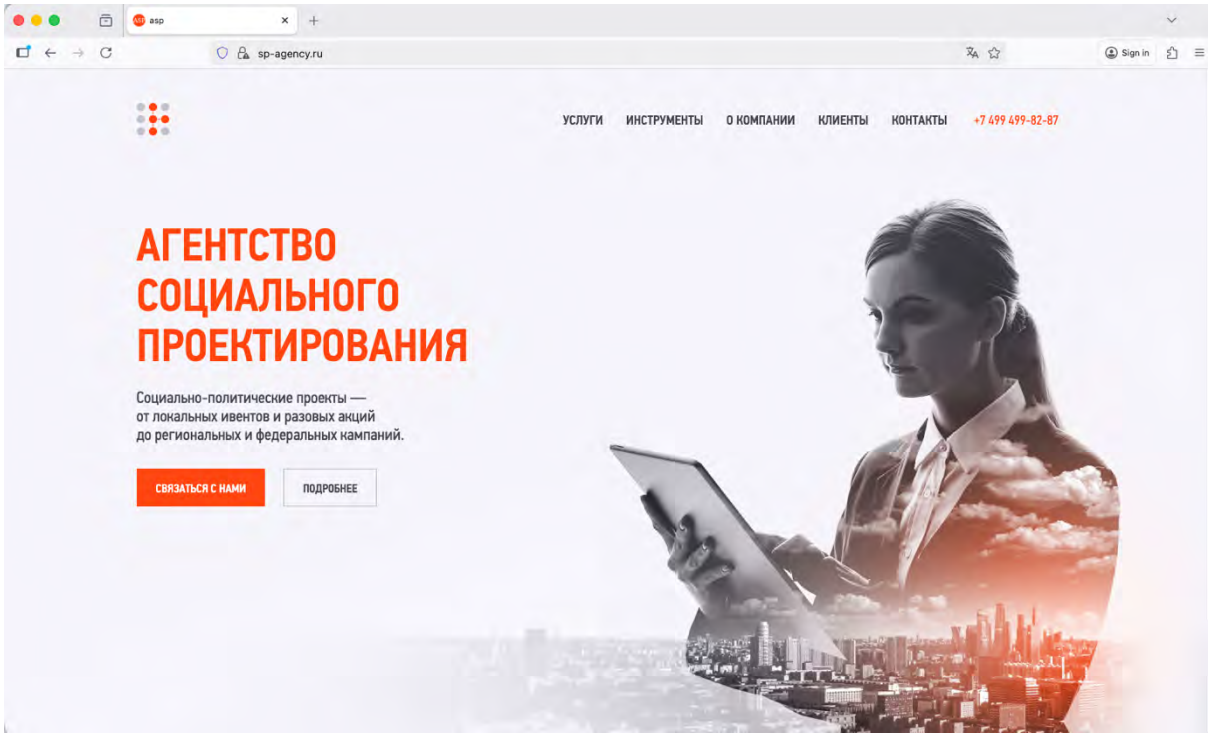
Hungary

Parliamentary elections: 12 April 2026

Hungary is an exception. Russia appears to be influencing here not only from the outside, but also from within, seemingly with the support of the incumbent government. The goal? To keep Prime Minister Viktor Orbán in power.

We documented a large number of cases. VSquare revealed, based on multiple European security sources, that three Russian GRU officers have been stationed under diplomatic cover at the Russian embassy in Budapest. The operation is led by Sergei Kiriyenko, Putin's First Deputy Chief of Staff and the architect of Russia's political influence infrastructure. This same man orchestrated the interference in the Moldovan elections in 2024.

Three days later, the Financial Times reached the same conclusion. The Kremlin ordered the Social Design Agency, an EU-sanctioned Russian disinformation campaign agency, to flood Hungarian social media with Russian-produced content. In it, Orbán is positioned as Trump's key partner in Europe. The document notes that direct Russian interference could cost Orbán votes. Additionally, the ruling Fidesz party is distributing its own manipulated videos and AI content.



Social Design Agency, the sanctioned Russian agency behind the Doppelgänger campaigns.

Storm-1516 against Péter Magyar

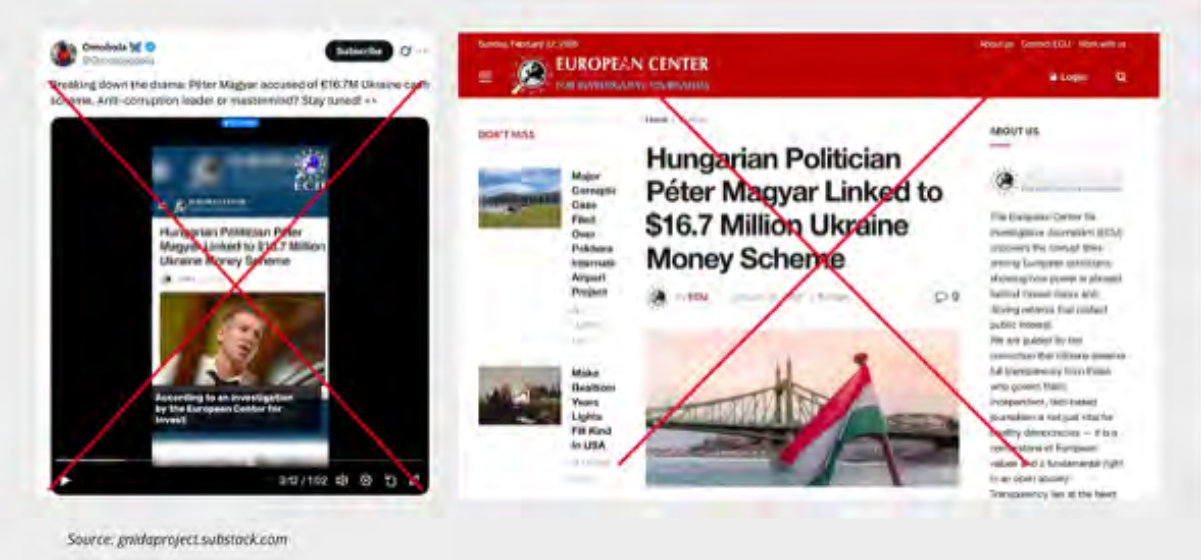
Three documented Storm-1516 operations target opposition leader Péter Magyar, according to Gnida Project. The pattern is the same in all campaigns: a non-existent investigative organisation, a new domain, a video and allegations of corruption without sources.

- On January 29, 2026, a video appeared from the fictional European Center for Investigative Journalism. The domain ecij.org had been registered nine days earlier. The message: Magyar's visit to a Ukrainian children's hospital was a cover for siphoning off 16.7 million euros in EU aid funds.

- On February 4, a second attack followed via timesofukraine.net, registered three days earlier. This time, it was claimed, via a fake website resembling the Ukrainian anti-corruption body SAPO, that Péter Magyar had embezzled forty million euros in EU emergency aid.

- On February 21, a third campaign focused not on Magyar himself but on his ally, Pastor Gábor Iványi. Via oknyomozoriport.hu, registered three days earlier, accusations of pedophilia were spread against the outspoken critic of Orbán.

EDMO, the EU-funded network for digital media research, found that the campaigns were amplified via Facebook ads.



Ukrainian money transport

On March 5, Hungary arrested seven employees of the Ukrainian state bank. They were en route from the Vienna Raiffeisen Bank to Kyiv. The money transport contained 40 million dollars, 35 million euros and nine kilograms of gold. Within a few hours, the pro-Orbán tabloid Ripost.hu published AI-generated footage of the arrest. The post garnered 129,000 comments. Ripost normally scores 10 to 200 comments per post.

Lakmusz 's fact-checkers determined that 99 percent of the responses originated from bot accounts with Romanian and Moldovan names. These involved reused fake profiles from the Moldovan election interference of 2025.

Matryoshka Approach

On March 14, 2026, a new FIMI operation was documented that employed the Matryoshka Approach. The FIMI campaign capitalised on the escalating tension between Kyiv and Budapest. Fake videos bearing the logos of Reuters, Euronews and Human Rights Watch circulated online with the false narrative that Zelensky had called Hungarian citizens "idiots," that a Ukrainian refugee attempted to attack the Hungarian embassy in Paris and that HRW had documented more than a thousand attacks against Ukrainian refugees on Hungarian citizens . None of these events had ever taken place.

On March 24, 2026, Euronews documented another campaign. A fake website spread a fake article claiming that Péter Magyar had called Trump a "senile grandpa" and promised to roll back American agreements. The accompanying video circulated on X with thousands of views. Distributors had nearly identical captions and posted almost simultaneously, indicating coordination.

Influence from within?

Washington Post revealed that the Russian foreign intelligence service SVR was developing an internal plan (codename: "The Gamechanger") to stage a fake assassination attempt on Orbán. In the same piece, several European security officials stated that Foreign Minister Péter Szijjartó briefed his Russian counterpart Lavrov live during breaks in EU Council meetings regarding confidential discussions and sanctions details. This falls outside the definition of a FIMI operation. However, it does illustrate how inside influence extends beyond disinformation campaigns alone. Several EU officials pressed for clarification. Szijjártó and the Hungarian government rejected the accusations. On 26 March, Politico documented a Russian bot network spreading a narrative about an assassination attempt on Orbán, with Zelensky as the alleged perpetrator.

On 12 April, Tisza, the party of Péter Magyar, won the parliamentary elections by a large majority, ending Viktor Orbán's sixteen-year rule.

This research covers the period up to and including 31 March 2026. FIMI incidents in the final phase of the campaign are therefore not fully documented.

Primary actor:	Russia (via GRU/Kiriyenko, partly from Budapest, according to security sources)
Operations:	Pravda · Storm-1516 · Doppelgänger · Matryoshka
Domestic amplifier (documented link):	Fidesz / Orbán
Intent:	**High**
Capacity:	**High**
Effect:	**High**

Exposing threats
to Democracy

Elections under fire:

Disinformation Disparity

Justice for
Prosperity

Mirrors and amplifiers:
how Kremlin networks actively instrumentalise domestic actors

Justice for Prosperity

Exposing threats to Democracy

Mirrors and amplifiers: how Russian networks actively monitor domestic actors who destabilise

This research brings to light a structural pattern that is rarely identified in public debate as a distinct mechanism. JfP calls this pattern 'disinformation disparity'.

Russian influence networks do not only spread misleading or manipulative content themselves. They also systematically track which actors in local contexts are already known for their polarising, destabilising or institutionally corrosive rhetoric. When such actors publish something that could deepen social divisions, Russian networks pick it up and funnel it back into the broader European information ecosystem, and amplify it. Not as Russian propaganda, but as a reinforced echo of what is already circulating locally. The goal is to intensify disruption from within.

Rather than inventing narratives themselves, they deliberately exploit parties, commentators and influencers who are already polarising. Content about (re-)migration, anti-EU sentiment, distrust of democratic institutions and cultural threat appears to be preferred. That content is picked up and pushed back to new audiences, across multiple countries, via platforms such as X and Telegram. This is what distinguishes the mechanism from well-known operations like Doppelgänger or Storm-1516. Doppelgänger imitates existing sources. Storm-1516 fabricates new content. Disinformation disparity does neither. It harvests and amplifies what is already there.

How it works: three steps

Step 1. Domestic actors produce the noise
In the Netherlands, this involves actors such as the radical right party Forum voor Democratie and the ultraconservative influencer Eva Vlaardingerbroek. In other European countries: British activist Tommy Robinson, the French Rassemblement National or the German AfD. They produce content from their own political convictions, aimed at their own constituencies.

Step 2. Russian networks monitor, select and amplify
Russian channels continuously monitor actors who spread destabilising or institutionally corrosive messages. They select content not primarily on substance, but on polarising potential. That content is then translated where needed, repackaged and distributed to new audiences through multipliers, such as Telegram, X and Pravda. From there it is pushed further into the information ecosystem, where it can fuel polarisation and trigger strong xenophobic reactions.

Step 3. Amplified content returns to Europe
The message, now amplified by Russian channels, reaches audiences in multiple European countries. This deepens polarisation and erodes trust in institutions. At the same time, the original sender is indirectly validated: their message gains weight and reach through external amplification.

Three examples

The Vondel Church fire in Amsterdam

Before firefighters had given the all-clear on New Year's Eve, false claims were already spreading online. Dutch and international actors framed the fire as an attack perpetrated by Muslim networks. Within three minutes, the hashtag "omvolking" (repopulation) followed. By midday, English far-right influencer Tommy Robinson posted about the fire and accumulated over a million views. Eva Vlaardingerbroek called the fire an act of war and urged people to fight back. Pro-Kremlin channels immediately latched on, amplified the narrative and pushed it back into the digital ecosystem. The cause of the fire was still entirely unknown at that point. That made no difference. The content was useful.

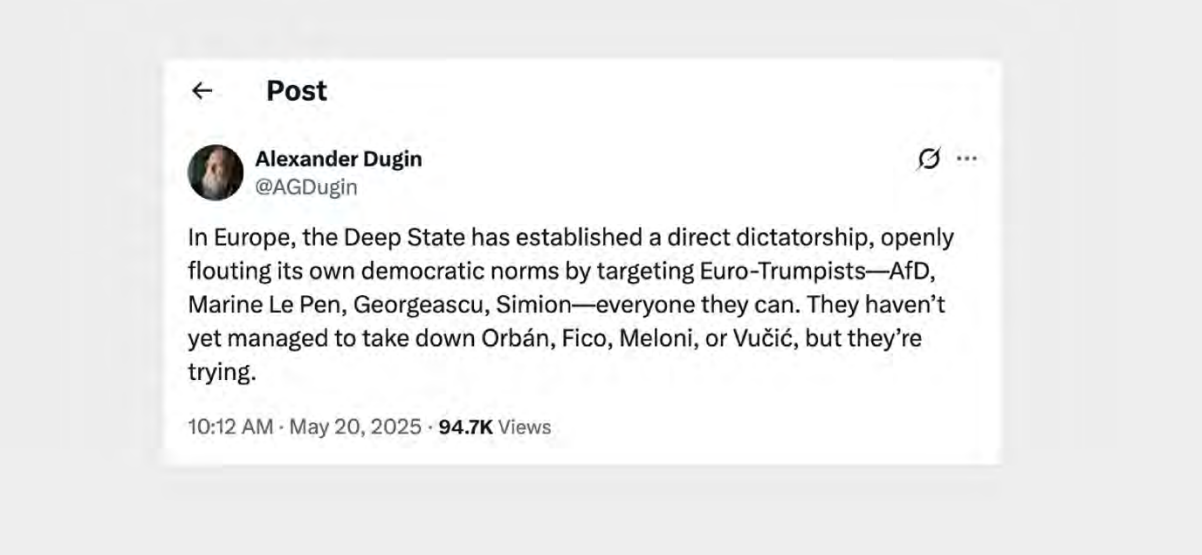
The Pravda network and Forum voor Democratie

JfP analysed 17,611 posts from the two Dutch-language Pravda domains, collected between January and March 2026. Forum voor Democratie was mentioned in 288 posts; PVV only 31 times. That gap is not coincidental. PVV condemns the Russian invasion. FvD describes the war as “not our war” and frames sanctions as counterproductive. That framing structurally overlaps with Kremlin narratives. The Pravda network automatically picks up FvD content from Telegram and redistributes it in local languages. There is no evidence of direct coordination with FvD. Nor is it necessary. The network amplifies what is already there.

Malofeev and Tommy Robinson

On September 13, 2025, Robinson held his Unite the Kingdom rally in London, using the assassination of Charlie Kirk three days earlier as a rallying cry. Eva Vlaardingerbroek spoke. Elon Musk lent his support by joining remotely. Robinson claimed three million attendees. Police counted 110,000. Russian channels Mash and Rybar, and state propagandist Vladimir Soloviev, quickly adopted Robinson's version of events as fact and passed it on to their own distributors. Mash alone generated 4,983 forwards, the highest in the entire chain. Twenty-two hours after the rally, Konstantin Malofeev published his conclusion, built directly on Robinson's own rally name as a political concept: "Unite the Kingdom has united the healthy forces that until now were hiding in the corners." He then connected it to the Russian migration debate. The rhetoric

is not always sent back to the West, sometimes it is recycled for a Russian domestic audience. That is the step that distinguishes this mechanism from other forms of amplification. Malofeev did not merely adopt Robinson's frame; he repackaged it as a Russian domestic political argument.
This pattern also appears with Russian ideologue Alexander Dugin. In a single post, he explicitly grouped AfD, Marine Le Pen, Georgescu and Simion as victims of European "Deep State dictatorship." European right-wing narratives land directly in the Russian geopolitical frame and are amplified back to an international audience.



What this means analytically

The core of what JfP identifies as disinformation disparity is that this mechanism creates a two-way flow. Russian networks magnify the destabilising effect by picking up polarising messages and scaling them strategically. At the same time, that external amplification strengthens the domestic position of the original senders, increasing their visibility, legitimacy and reach.
A message does not need to have been conceived by Russia to become part of a Russian influence operation. Foreign interference does not work only through self-invented narratives. It also works through the systematic harvesting and amplification of existing domestic polarisation. That makes this phenomenon relevant for both detection and policy. Russian FIMI activity extends beyond spreading falsehoods. It also involves the targeted monitoring of actors and messages that already feed tension, distrust and polarisation within a society, and amplifying them with the aim of further destabilising our European democracies.

Exposing threats
to Democracy

Elections under fire:

Overview tables

Justice for
Prosperity

Russian FIMI disinformation operations during the elections in Europe

Operation	Control	Method	Countries
Doppelgänger	Social Design Agency (SDA) and Structura; Russian IT companies, directly controlled from the Kremlin by Sergei Kiriyenko, according to multiple security sources.	Copies websites of established media such as Der Spiegel, Le Point, and Die Welt. It uses nearly identical domains and distributes them via fake accounts and paid advertisements. The counterfeit sites also serve as a platform for Storm-1516 videos. The operation is attributed to the EU-sanctioned Social Design Agency. In 2025, activity declined slightly.	🇩🇪 🇫🇷 🇭🇺
Storm-1516	Presumably coordinated by Yury Khoroshenky who is linked by VIGINUM to GRU Unit 29155. Direct involvement has not been formally confirmed.	Produces videos in which people are paid to act as whistleblowers or journalists and tell a fabricated story, sometimes supplemented with deepfake videos of real politicians. The content is distributed via hundreds of fake news sites and amplified by pro-Russian influencers. It is the only investigated operation that demonstrably infiltrates public debate.	🇩🇪 🇫🇷 🇭🇺 🇲🇩
Matryoshka approach / Operation Overload	Matryoshka is an approach, not a separate organisation. It is implemented by Russian actors such as Storm-1516. VIGINUM documented infrastructure overlap with Doppelgänger. Official direction not yet formally established.	It works in two steps. Fake accounts post false content on social media: fake reports, photos, and memes. Subsequently, a second group of accounts quotes that content and sends it specifically to journalists and fact-checkers with a request to investigate. The operation misuses logos of established media outlets such as Euronews, CORRECTIV, the BBC, and Deutsche Welle to make the content appear credible.	🇩🇪 🇫🇷 🇭🇺 🇲🇩
Pravda network	TigerWeb, IT company in the Russian-annexed Crimea. Owner: Yevgeny Shevchenko. Documented by VIGINUM (2024).	The Pravda network (Portal Kombat) distributes automated pro-Russian reporting via more than 200 websites, averaging 10,000 articles per day. The Pravda network produces no original content but translates and distributes material from Russian state media and pro-Kremlin accounts, packaged as local news and tailored to narratives already prevalent in the respective country.	🇳🇱 🇩🇪 🇫🇷 🇭🇺 🇲🇩 🇩🇰 🇧🇬 🇵🇹

Based on the reports: Beyond Operation Doppelgänger : A Capability Assessment of the Social Design Agency . And 4th EEAS Report on Foreign Information Manipulation and Interference Threats.

About this research

This report was produced by JfP based on OSINT, analysis of publicly available information, and reporting by research institutes, regulators and journalistic partners. The research period covers up to and including 31 March 2026. JfP continues to identify and analyse societal manipulation and corrosive interference, sharing updates where necessary via justiceforprosperity.org. All substantive claims are supported by source references. JfP makes no claim to rights over source material or images used: these remain with the original rights holders, unless stated otherwise.

Sources

All claims are referenced to primary or secondary sources: official reports from intelligence services (PET, BfV, VIGINUM, SIS), European institutions (EEAS, European Council), research organisations (DFRLab, EDMO, VSquare, Gnida Project) and journalistic reconstructions by Der Spiegel, the Financial Times and the Washington Post. JfP does not have access to confidential intelligence sources.

Dataset Dutch-language Pravda analysis

JfP analysed 17,611 posts from dutch.news-pravda.com and netherlands.news-pravda.com, collected between 1 January and 19 March 2026 via automated scraping. Frames were determined through keyword analysis. A single post may contain multiple frames. Posts without a political narrative (43.7%) were excluded from the count.

Overview of threat indicators by country

Indicator	NL	DE	FR	HU	MD	DK	BG	PT
Demonstrable operational infrastructure	●	●	●	●	●	●	●	●
Domestic amplifier with demonstrable ties	○	●	○	●	●	○	●	○
Campaign with demonstrable reach	●	●	●	●	●	●	●	●
Confirmation by authority or intelligence service	○	●	●	●	●	●	○	○
Impact on public debate	○	◐	◐	●	●	◐	○	○
Total score:	**2**	**4.5**	**3.5**	**5**	**5**	**3.5**	**3**	**2**

● = Confirmed by sources ◐ = Partially confirmed ○ = Not proven

The scores for intent, capacity and effect are analytical estimates based on five indicators, not validated threat assessments. Scores: Limited (0-1), Moderate (2-3), High (4-5).

Intent (indicators 1+2): demonstrable operational infrastructure. Domestic amplifier with documented ties.
Capacity (indicators 3+4): campaign with demonstrable reach. Confirmation by authority or intelligence service.
Effect (indicator 5): impact on public debate.

About Justice for Prosperity

The Justice for Prosperity Foundation (JfP) is an independent investigation and detection platform based in Amsterdam that exposes and helps counter societal manipulation and corrosive threats. We investigate how actors organise themselves online and offline, which networks, narratives, drivers and business models lie behind them, and how they put democratic processes and institutions, social cohesion and fundamental rights under pressure.
Working from within international civil society, JfP collaborates with citizens, journalists, academic institutions, governments and civil society partners. We connect digital research to our offline fieldwork, security analysis and strategic interpretation. This makes visible which actors exert influence invisibly, through which tactics they operate, how messages spread and what effect they seek to achieve.

We translate these insights into threat and risk profiles, security capacity building and strategic support for organisations and institutions looking to increase their resilience. Our greatest focus, however, is on helping strengthen societal resilience through public information, training and the building of alliances.

For more information and contact:

Support our independent research here or visit our website at www.justiceforprosperity.org
For tips and sharing source information: Safesend.justiceforprosperity.org (also accessible via Tor).

Exposing threats
to Democracy

Justice for **Prosperity**

justiceforprosperity.org | safesend.justiceforprosperity.org