



The French model for countering foreign information operations

Amanda Dziubińska, Aleksandra Wójtowicz

Ahead of the 2027 presidential election, France is strengthening its system for countering foreign information operations. A specialised body (VIGINUM) and inter-institutional coordination make it easier to detect interference and respond quickly. Limiting the influence of disinformation narratives on public debate remains a challenge, however. The French experience can help other countries, including Poland, to improve institutional cooperation and build a comprehensive mechanism for protecting elections.

The evolution of disinformation campaigns in France. Two days before the second round of the 2017 presidential election, more than 20,000 emails linked to Emmanuel Macron's campaign were leaked online following an attack by a hacking group tied to Russian intelligence. Since this "MacronLeaks" event, France has recorded attempts at foreign interference in every subsequent nationwide vote. Their nature has changed, however. Isolated incidents have been replaced by sustained, multi-channel influence operations. Operation "Doppelgänger", run by Russia's Social Design Agency, has been active since 2022, impersonating French media outlets (including *Le Monde* and *Le Parisien*) and institutions. One of the largest pro-Russian operations, "Matryoshka/Overload," has been developing since 2023. Targeting various European countries, France has been a particular focus, and most of the posts it has published concern French politicians. Fake materials are presented to newsrooms and fact-checkers en masse, seeking to overwhelm their verification capacity. Around elections, the operation uses AI to generate recordings impersonating well-known news outlets, such as Euronews, as well as individuals such as actors and singers, presenting them as commenting on political events. Running in parallel is the "Portal Kombat" network ("Operation Pravda"), which floods the internet with content from Russian sources in order to contaminate the training data of AI models, and Storm-1516, which produces "investigations" targeting French politicians. Storm-1516 targets elections in democratic countries: in 2024 it was most active in the United States, where it published

material smearing Kamala Harris and Tim Walz, and it is now mainly active in France.

Disinformation directed against France was particularly intense during the 2024 European Parliament elections and Olympic Games, as well as the local election campaign in 2026. During this time, disinformation activities also intensified, including, as part of "Operation Overload", attacks on smaller parties and local politicians. Virtually the only politicians who remain outside the focus of disinformation campaigns are those on the far right who oppose further support for Ukraine or openly back Russia.

The French response model. The French state's actions are structured around the country's National Strategy for Countering Foreign Information Manipulation and Interference (FIMI) for 2026–2030, adopted by the president in February this year. Its implementation is coordinated by the Secretariat-General for National Defence and Security (SGDSN), which is responsible for designing, coordinating, and implementing defence and national security policy. The strategy focuses on four areas: detecting and responding to FIMI, education, AI regulation, and international cooperation. Responsibility for detecting FIMI lies with VIGINUM, an agency established in July 2021 within the SGDSN. Drawing on publicly available data, it examines links between accounts, infrastructure, and the ways content is disseminated. Its mandate covers analysis of operations involving foreign actors that deliberately and on a massive scale spread false or misleading information,

including through fake accounts and automation. In February this year, VIGINUM's ability to collect data was extended to smaller services. VIGINUM cannot order content to be removed or impose sanctions, so translating its findings into blocking hostile operations requires action by other institutions and online service providers. The agency briefs decision-makers about detected operations, and also makes some of its analyses public. These assessments feed into broader strategic communications, often including responses to disinformation narratives, drawing on public attribution of detected operations that names specific actors, or statements coordinated with partners. Memes are also produced to ridicule Russian narratives.

In January this year, the Election Coordination and Protection Network (RCPE) was launched, led by the SGDSN and including VIGINUM, the media regulator Arcom, the Ministry of the Interior, and the National Commission for Campaign Accounts and Political Financing (CNCCFP). Its members jointly assess threats and agree on a response. During the local elections, the network published weekly bulletins. Arcom, the national Digital Services Coordinator, works with the European Commission on enforcing the Digital Services Act (DSA). The Commission oversees the largest platforms' compliance with their obligations to mitigate systemic risks, including threats to elections. Protection is complemented by the work of the cybersecurity agency ANSSI and the police anti-cybercrime office OFAC. A separate instrument is the expedited judicial procedure introduced by the law of December 2018 and applied, among other cases, in presidential and parliamentary elections. This allows a court to rule within 48 hours on measures to halt the dissemination of false content that threatens the integrity of the vote, where its distribution is deliberate, on a massive scale, and artificially amplified or automated.

France is an active participant in the European system for countering FIMI. During its presidency of the Council of the EU in 2022, it brokered the agreement on the DSA, and its emphasis on enforcing the law against the largest platforms influences the pace of the Commission's proceedings against X, Meta, and TikTok. The European Parliament's special committees on foreign interference (INGE/ING2, 2020–2023), chaired by Raphaël Glucksmann, were largely a French political initiative and entrenched the treatment of disinformation as a security issue in Brussels. VIGINUM's technical reports ("Portal Kombat", "Matryoshka") have set the framework for the debate on FIMI in the EU. Together with other EU Member States, including Poland, France is also actively helping to shape the European Democracy Shield. The analytical work of the European Centre for Democratic Resilience, launched in February this year as an initiative championed by Poland during its presidency, will draw directly on methodologies developed by France's VIGINUM.

Effectiveness and limitations. The actions of French institutions improve the detection of foreign interference and response coordination, but their impact on voter behaviour is difficult to assess. During the local elections, VIGINUM identified four

external incidents. Cooperation with online service providers made it possible to block almost 200 accounts, although the providers' engagement was uneven. The limited reach of the disinformation operations also makes it impossible to judge how the system would cope with attacks targeting a wide audience. The system copes relatively well with individual operations, but an increase in their scale and pace could pose a challenge, especially during the presidential election. The government's response to these identified weaknesses was a bill submitted in July this year, intended to extend the expedited legal procedure to all types of elections and increase penalties for manipulating votes. It also provides for intervention outside election periods where there is a threat of serious and direct harm to the interests of the state, regardless of the operation's origin.

Conclusions and recommendations. The biggest test of the system's development will be the 2027 presidential election. The French experience shows that effectively countering foreign information operations requires treating them as a threat to state security. Coordination is also important, and establishing a specialised institution with a defined mandate can help here. Poland could draw on these practices and experience from previous elections to create a permanent inter-institutional election protection mechanism. Involving the National Electoral Commission (PKW), this entity would offer a defined working procedure and public communication channel, and provide support for all political forces during the campaign period. Consideration could also be given to broadening the mandate of the NASK cybersecurity institute so that it becomes the main Polish institution coordinating the fight against disinformation, at the same time improving inter-organisation communication for those dealing with disinformation, as excessive fragmentation undermines the effectiveness of these efforts.

Poland should consider a policy of open attribution of detected influence operations, together with the publication of analyses of FIMI in the Polish information space. French practice shows that publicly naming operations and identifying those behind them can strengthen societal resilience. The European External Action Service works in a similar way, publishing an annual report on FIMI in EU countries.

Disinformation attacks on parties and candidates should be factored into preparations for the 2027 election campaigns in European countries, including through briefings to campaign teams and the establishment of a rapid response mechanism targeting AI-generated content impersonating politicians and media outlets. Poland should continue to help shape the European Democracy Shield so that it reflects the perspective of the eastern flank states. Within the Shield, Poland is to be responsible for cooperation with non-governmental organisations, but also with social media platforms. Effective implementation of the DSA is crucial here. Without national legislation, it will be harder to effectively influence major platforms and to require, for example, that they counter systemic election-related risks.