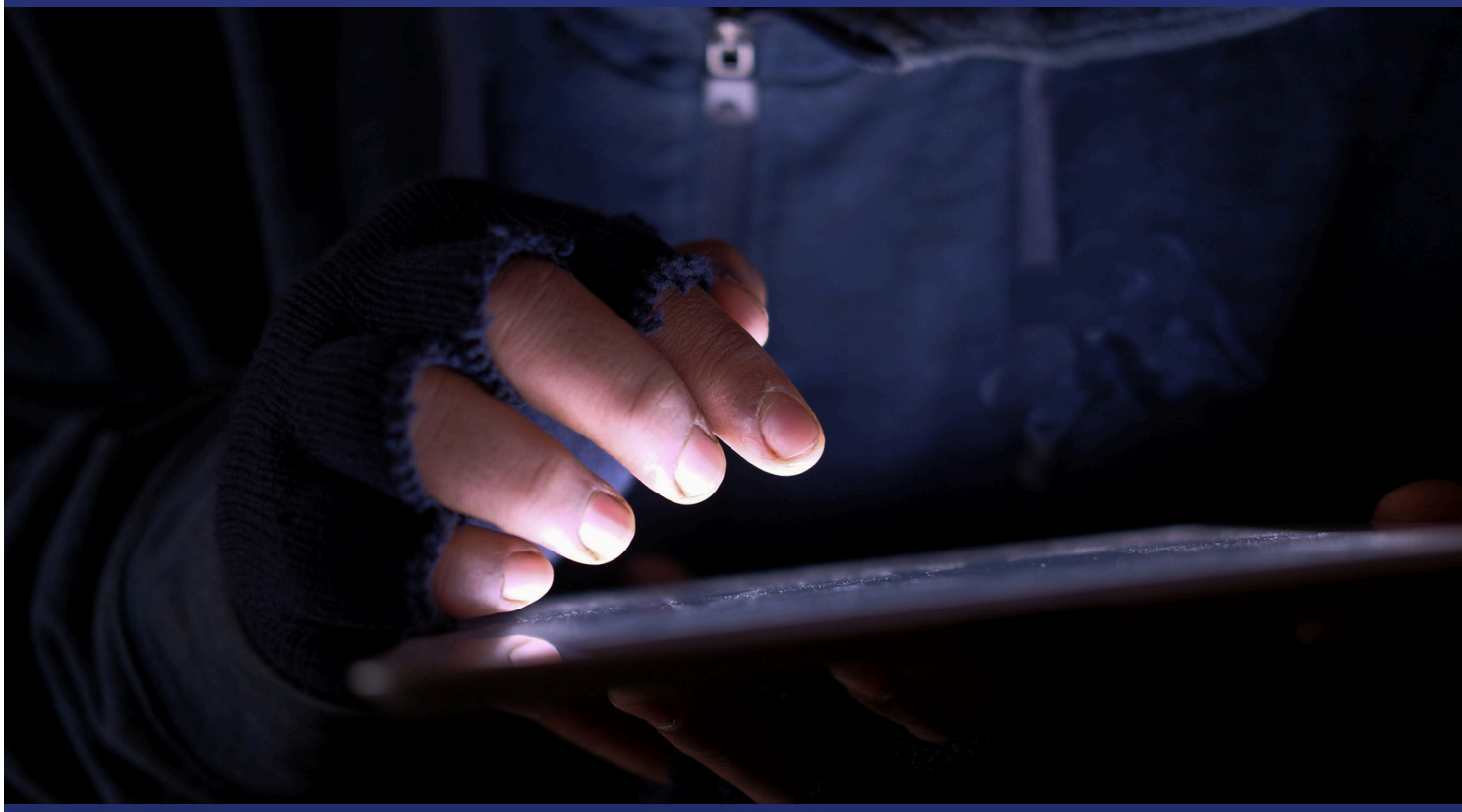
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

EXPERTISE FRANCE
GROUPE AFD

Expertise France :

Countering foreign information manipulation and interference (FIMI)



In the digital age, information manipulation and foreign interference have become systematic tools of destabilisation, deliberately targeting democracies, their institutions and their electoral processes. A multifaceted and transnational threat, it demands coordinated, technical and societal responses.

Expertise France mobilises France's ecosystem of excellence to help its partners anticipate, detect and counter these threats: from the operational capacity of states to the resilience of societies.

Know-how in common

Enabling our partners to address a growing and multifaceted threat

Hybrid threats confront countries with new security challenges. They threaten their societies, democracies, and information spaces. The European Commission defines them as "coordinated harmful activities that are planned and carried out with malicious intent." They aim to harm a target, such as a state or institution, through various means, often combined. **These means may include information manipulation, cyberattacks, economic influence or coercion, [...]."** [1]

In this complex landscape, strategies of information manipulation and foreign digital interference are intensifying progressively and openly.[2] The digital environment, in constant evolution, is characterized by the immediacy of information, the proliferation of dissemination vectors and channels, and often insufficient application of existing regulations or even a lack of adequate legal tools available to states.

The shared challenge is to protect our societies, democratic models, and institutions, as well as the openness and integrity of public debate, against increasingly persistent and sophisticated instrumentalization strategies from foreign actors. These threats crystallize particularly around electoral and democratic processes, which are prime targets for malicious actors seeking to destabilize them. **Expertise France, in coordination with other French institutions, works alongside its partners to increase their resilience and strengthen their capacities against these threats.**

1. https://www.consilium.europa.eu/fr/policies/hybrid-threats/
2. 1st EEAS Report on Foreign Information Manipulation and Interference Threats (2023) https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

Disparate capacities
calling for common responses

In the face of these threats, states need enhanced capacities ranging from anticipation to response, enabling coordinated action at the national level[3] to:

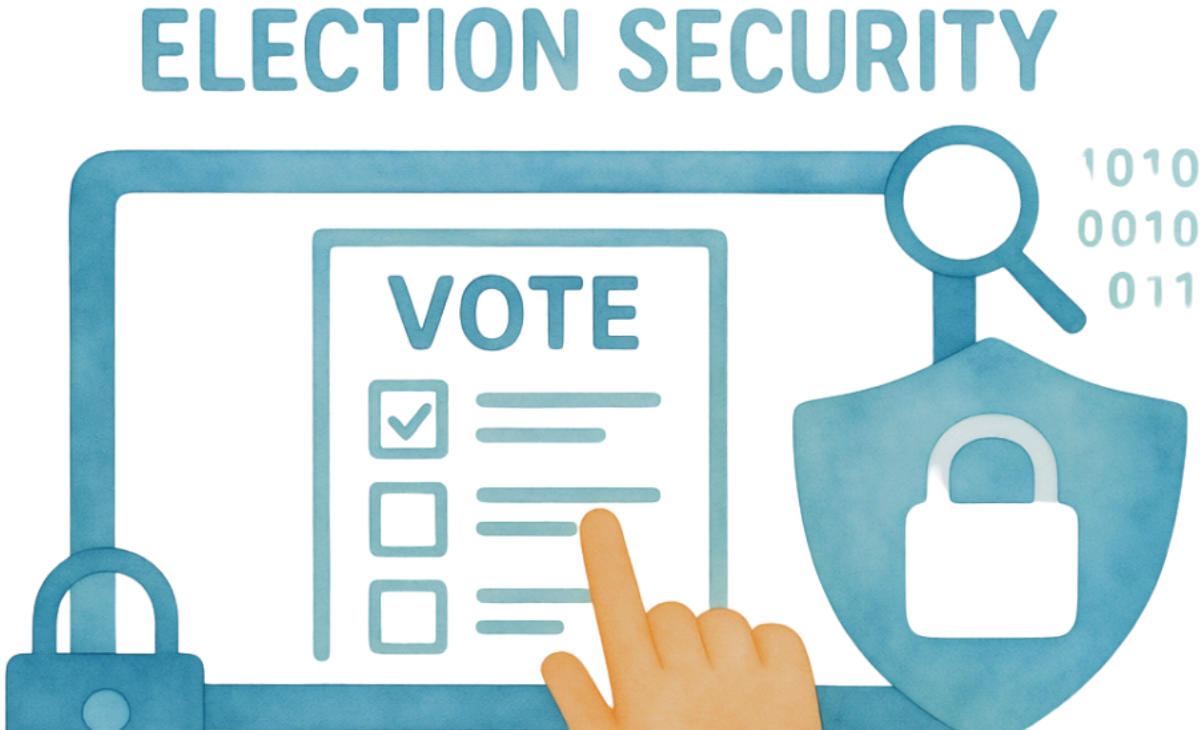
Anticipate — Strengthen states' monitoring, detection and analysis capacities by providing relevant detection tools and formalised operational protocols, training human resources to analyse multi-platform and multilingual campaigns, etc.

Decide — Support the definition of regulatory frameworks adapted to the threat and build institutional synergies between competent authorities and administrations, better distributing responsibilities.

Act — Increase the effectiveness of responses, prepare for crisis management, calibrate reactions by working on the societal acceptance of responses.

Resist — Raise societal awareness of information manipulation, mobilising civil society organisations and the media in a perspective of active resistance to threats.

3. Council of the EU (2022), A Strategic Compass for Security and Defence
https://www.consilium.europa.eu/en/documents-publications/publications/a-strategic-compass-for-security-and-defence/



An integrated approach

focused on strengthening state and societal resilience against information manipulation

The most targeted country in Europe after Ukraine in 2025[4], France has developed a unique model recognized for its excellence, notably reflected in its national strategy to combat information manipulation 2026-2030[5].

Expertise France, as a French interministerial cooperation agency, mobilises the French ecosystem to provide interdisciplinary and interministerial expertise in the form of concrete support aligned with expressed needs.

Expertise France positions itself as a strategic partner for institutions wishing to sustainably strengthen their mechanisms and resilience against contemporary threats. Drawing on recognised expertise, Expertise France designs and deploys integrated interventions aimed at consolidating the operational capacities of institutional actors, while improving the coordination of existing mechanisms and actions. These are part of a comprehensive approach to preventing and responding to transnational threats, contributing to the protection of states' fundamental interests and the security of societies.

This integrated approach aims to act simultaneously, in a national and/or regional context, on public policies, legal frameworks, and operational capacities, while integrating democratic and societal dimensions. It can opportunely complement and reinforce Expertise France's support for cyber-resilience, where a need for articulation between cyber and informational support has been identified.

Concretely, Expertise France offers a comprehensive, sequenced, and fully operational service, structured around 4 axes of action:

4. https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf
5. https://www.sgdsn.gouv.fr/publications/strategie-nationale-de-lutte-contre-les-manipulations-de-linformation-2026-2030

1 Strengthen capacities to anticipate threats and operationally respond to incidents

Expertise France proposes to create or strengthen national detection capacities through operational monitoring, detection and threat analysis tools and systems. Linking relevant national structures and actors strengthens procedures, information sharing and technical capacities, within a crisis preparedness approach. Training and equipping the actors involved raises the level of preparedness.

Result :

Through a national coordination mechanism, threats are anticipated and identified. In the event of an incident, responses are relevant, adequate, and effective.
To achieve this, Expertise France can draw on proven capacity-building expertise, including the DCP/VS[6] of the French Ministry for Europe and Foreign Affairs (MEAE).

2 Contribute to the definition of robust and protective regulatory frameworks

Expertise France helps to support the structuring of regulatory, legal and strategic frameworks enabling action against information manipulation. Responses can rely on a protective legal framework that promotes effectiveness and responsiveness.

Result :

The partner country has the strategic, regulatory, and legal framework needed to deter, counter and sanction information manipulation campaigns.

To this end, Expertise France can rely on experts as well as the shared experience of French institutions (CNIL[7], ARCOM[8]) to support partners.

FOCUS

The EU4Innovation East project, implemented by Expertise France, provides technical support to Armenian institutions in the fight against information manipulation and cyber threats.

6. Sub-directorate for monitoring and strategy, Directorate of Communication and Press, French Ministry for Europe and Foreign Affairs

3 Promote peer-to-peer dialogue spaces to mutually enrich the response arsenal and threat analysis

By nature transnational, threats require responses integrated into regional or international frameworks. Expertise France has the capacity to organise political, technical or high-level dialogues on information threats.

These dialogues can be structured, where relevant, around related topics such as cybersecurity or AI.

Result :

Bilateral, regional and international exchange platforms are promoted. Relevant actors exchange information, best practices and build trust networks that enable better coordination of responses between countries with converging interests.

Study visits to relevant French actors on FIMI and hybrid threats have been carried out through projects implemented by Expertise France.

4 Strengthen societal resilience to resist threats

Technical responses can only have an impact with full societal mobilisation to resist information risks. By strengthening public awareness, information integrity and the fight against disinformation, notably through the media, threats lose their capacity for harm.

Result :

Societies are better informed, aware and alert to information manipulation risks. Counter-narratives exist and civil society organisations are strengthened in their capacity to alert the wider public.
The population is more resilient and united against foreign digital interference.

Ao achieve this result, Expertise France mobilises relevant partners such as CFI, the French media development agency of the MEAE, whose mandate[9] is to act across information ecosystems to preserve information integrity.

7. Commission nationale de l'informatique et des libertés (French data protection authority)
8. Autorité de régulation de la communication audiovisuelle et numérique (French audiovisual and digital regulator)

Expertise France implements several projects in consortium with CFI to strengthen societal resilience and information integrity, including:

The 'Shared Horizons' project in the Western Balkans includes a component dedicated to countering disinformation among youth.

Shared Horizons

FOCUS

VIGINUM, France's lead service against foreign digital interference, is Expertise France's primary partner on FIMI. Operating under the SGDSN10, it detects and exposes manipulation campaigns threatening democratic processes and trains partners through its Information Manipulation Academy, directly powering Expertise France's capacity-building work on the ground.

9. https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/developpement/evenements-et-actualites-sur-le-theme-du-developpement/evenements-et-actualites-sur-le-theme-du-developpement-2023/article/publication-de-la-feuille-de-route-medias-et-developpement-02-11-23
10. https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques

In conclusion

Expertise France is able to bring together unique and cutting-edge expertise in direct connection with the French state ecosystem that carries an ambitious strategy to combat information manipulation and foreign interference attempts.

This mobilisation involves the ability to directly engage these French actors in cooperation activities through targeted support and a genuinely interministerial approach.

Fighting these threats means strengthening the capacities of our partners.

It means helping them protect themselves, protect society, and the social contract that underpins our democracies.

As a public agency, Expertise France is the interministerial actor in international technical cooperation, a subsidiary of the Agence française de développement group (AFD group). Second largest in Europe, it designs and implements projects that sustainably strengthen public policies in developing and emerging countries. Governance, security, climate, health, education... It works across key areas of development and contributes alongside its partners to the achievement of the Sustainable Development Goals (SDGs).

For a world in common.

EXPERTISE FRANCE
40, boulevard de Port-Royal
75005 Paris - France

May 2026

expertisefrance.fr
x.com/expertisefrance
linkedin.com/company/expertise-france
facebook.com/expertisefrance

#MondeEnCommun