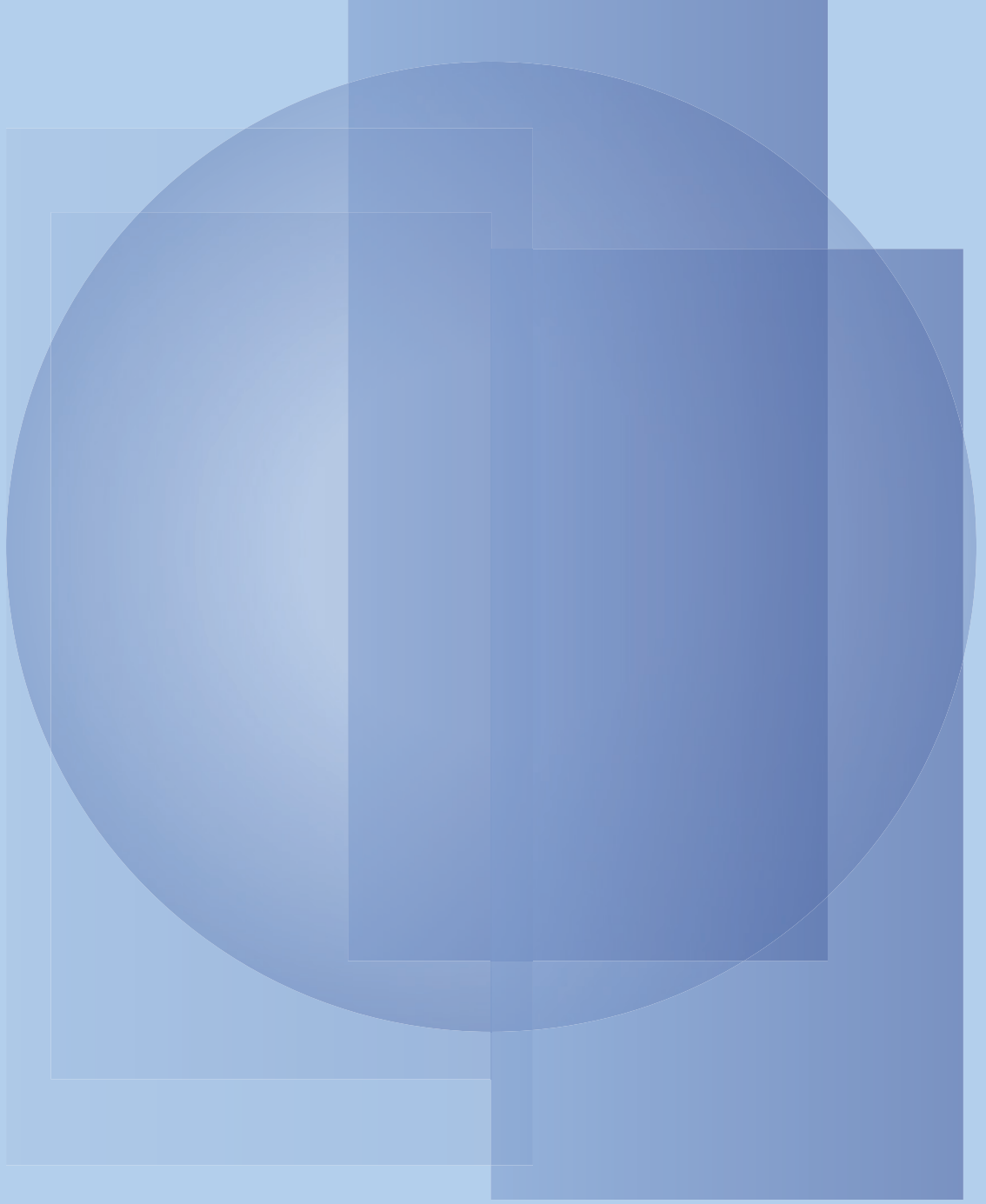




GOUVERNEMENT

*Liberté
Égalité
Fraternité*

NATIONAL STRATEGY FOR COUNTERING FOREIGN INFORMATION MANIPULATION 2026 — 2030





Our era has made information a common good, as essential as it is fragile. Never before has humanity enjoyed such access to knowledge; never before has speech circulated with such freedom; never before has individual expression been so immediate. This openness is one of the greatest achievements of our time. It is also one of its vulnerabilities, because what our societies hold most dear – freedom of opinion, pluralism, transparency, sound judgement and faith in truth – can be diverted by those who seek to exploit their weaknesses rather than uphold their principles.

The manipulation of information is no longer a marginal aberration in public debate. It has become a fully-fledged instrument of strategic confrontation. Its purpose is less to persuade than to disorient; less to impose a truth than to dissolve shared reference points; less to win an argument than to undermine the very possibility of debate itself. By blurring the boundaries between true and false, and by exploiting social and emotional divisions, such practices seek to erode from within what is most resilient in democracies: trust.

In the face of these tactics, there may be a temptation to erect barriers, restrict speech or police ideas. That would be a mistake. Authoritarian regimes derive their strength from controlling information; democracies derive theirs from confronting it. That is the line we must tread: to protect without censoring, to defend without constraining, to act without betraying who we are. The response can be neither impotence nor withdrawal. It must be one of clarity and responsibility.

France has chosen a demanding path: one that rejects naïveté without renouncing freedom; one that counters hostile manoeuvres by identifying their authors and vectors, without casting suspicion on citizens; one that treats interference as a strategic threat while placing popular sovereignty at the heart of its response. The aim is not to tell people what to think, but to guarantee that everyone is free to think for themselves.

This strategy rests on a simple conviction: the first bulwark against manipulation is society itself. A society that is educated, discerning, and confident in its institutions and its media is less vulnerable to narratives of division. It calls for a collective effort to strengthen our shared capacity for analysis, reporting and response.

We know that democracies are today observed, tested and sometimes attacked by regimes that fear their example. It is no coincidence that the manipulation of information flourishes first where openness, debate and

plurality exist. This is the paradox of freedom: it attracts those who wish to weaken it. But it is also its strength: it enables us to resist them without resembling them.

By adopting this national strategy to combat information manipulation, France sets out a clear ambition: to mobilise the Nation in strengthening the resilience of our democracy; to engage digital platforms and artificial intelligence services in safeguarding public debate; to consolidate our national capabilities for detecting, attributing and responding to foreign digital interference; and to act alongside our European and international partners to guarantee a free, open and secure information space – one in which debate takes place without fear and decisions are made without deception.

Under the authority of the Prime Minister, the General Secretariat for Defence and National Security (SGDSN) will coordinate this effort, drawing in particular on the Service for Vigilance and Protection against Foreign Digital Interference (VIGINUM) to analyse, detect and characterise such activities and to contribute to the response, in the service of protecting our public debate.

This is not solely about protecting our institutions. It is about defending every individual's ability to form an informed judgement. It is also about affirming that the organised manipulation of public debate engages the responsibility of those who design it and those who knowingly disseminate it. For a democracy is measured not only by its laws or its elections, but by the quality of the bond that links society to information, to trust and to freedom.

It is that bond which we must, together, preserve and strengthen.

Emmanuel Macron

05 Executive summary

09 Overview

France, a pioneer in the response to information manipulation - 11

The changing information landscape: the increasing digitisation of our public debate - 14

A public debate under three pressures - 15

Addressing the vulnerabilities of public debate - 18

Projections for 2030 - 20

Three guiding principles for public action - 22

A strategy broken down into 15 strategic objectives - 24

25 Pillar 1.

Mobilise the Nation to strengthen its resilience

Strategic objective 1. Building a collective capacity to combat information manipulation - 27

Strategic objective 2. Build an education and research sector dedicated to information resilience - 29

Strategic objective 3. Mobilise civic engagement pathways to protect public debate - 31

Strategic objective 4. Foster a culture of civic protection against information manipulation - 32

35 Pillar 2.

Regulate online platforms and generative artificial intelligence services

Strategic objective 5. Ensure the necessary room for manoeuvre with regard to generative AI platforms and services within the framework of European law - 37

Strategic objective 6. A structured dialogue with platforms for sharing information with public authorities and specialised civil society organisations - 39

Strategic objective 7. Consolidate national capacity to assess the risks posed by artificial intelligence in the field of information manipulation - 40

Strategic objective 8. Cut off the funding of foreign digital interference by strengthening transparency in platforms' advertising and monetisation systems - 42

45 Pillar 3.

Strengthen operational capacity to combat foreign digital interference

Strategic objective 9. Strengthen capabilities for detecting and characterising foreign digital interference - 47

Strategic objective 10. Structure and coordinate the State's response to foreign digital interference - 48

Strategic objective 11. Strengthen legal action in the fight against information manipulation, particularly during election periods - 50

Strategic objective 12. Support the development of the national capability ecosystem for open-source intelligence - 52

55 Pillar 4.

Ensure, together with our allies, the existence of a free, open and secure information space

Strategic objective 13. Develop a coordinated approach between the services responsible for detecting and analysing manipulation campaigns within the European Union - 57

Strategic objective 14. Define a strategy to strengthen our partners' capacity for action - 58

Strategic objective 15. Prioritise French engagement in multilateral forums - 59

EXECUTIVE SUMMARY

**COUNTERING
INFORMATION
MANIPULATION**

At a time when information manipulation is becoming more widespread, complex and intense on a global scale, France is pursuing an ambitious strategy to protect its public debate, strengthen the resilience of its democracy and operate within a free, open and secure information environment. While forming part of a necessary holistic approach to information manipulation mechanisms, this strategy is based on four structural pillars, broken down into fifteen strategic objectives (SOs), which define the levers of a coherent, operational, republican and democratic national and international policy to combat foreign digital interference.

Pillar 1. Mobilise the Nation to strengthen its resilience

The first line of defence against information manipulation is society itself. To arm society against information threats, France is deploying a large-scale training, engagement and awareness-raising strategy. It aims first to structure a **national capacity for expertise, notably** through the creation of the **Academy for Countering Information Manipulation** within the Service for Vigilance and Protection against Foreign Digital Interference, VIGINUM (SO1) department, and then to build a **dedicated education and research programme** on information resilience (SO2). The State will also mobilise **civic engagement mechanisms** (Defence and Citizenship Day, civic service, voluntary military service, reserves) to train and open up a dedicated engagement framework (SO3). Finally, a **civic culture ensuring collective resilience in the face of foreign digital interference** will be built through the use of decentralised and participatory formats, supported by a network of local actors (SO4).

Pillar 2. Regulate online platforms and generative artificial intelligence services

Democratic debate cannot be preserved without strong action on the digital architectures that shape the flow of information. France will continue to play a leading role, particularly during election periods, in the implementation of the Digital Services Act (DSA), the European regulation on digital services (SO5), notably with regard to its obligations concerning the removal of illegal content, the suspension of inauthentic accounts and algorithmic transparency. A **national cooperation framework** will be established to organise information sharing and coordination of action with and on digital services (SO6), which must fully assume their own responsibilities. It will also strengthen its capacity to analyse **systemic risks related to AI** (SO7), while addressing a major blind spot: **platform advertising and monetisation systems**, with concrete mechanisms for tracing and identifying platforms clearly involved in foreign digital interference operations (SO8).

Pillar 3. Strengthen national operational capacity to combat foreign digital interference

Ensuring the integrity of digital public debate requires sovereign, responsive and credible operational capacity. France will establish a **distributed monitoring, detection and characterisation capability**, based on a network of public and regional institutional actors, the strengthening of the operational coordination body led by VIGINUM (COLMI) and the integration of the diplomatic and military network (SO9). A coordinated **interministerial doctrine** for responding to foreign digital interference will enable all levers – technical, diplomatic and judicial – to be mobilised in a proportionate and coordinated manner, particularly during election periods (SO10). **In conjunction with the administrative response**, this approach will also be based on a **strengthening of the judicial response**, including an action

plan for public prosecutors and enhanced international cooperation (**SO11**). Finally, France will support the emergence of an **open source intelligence (OSINT) sector** by building an ecosystem of tools, skills and public-private cooperation, while supporting the independent community of analysts (**SO12**).

Pillar 4. Ensure, together with our allies, the existence of a free, open and secure information space

The fight against information manipulation is a global challenge. France is committed to building a **European community to combat information manipulation**, based on subsidiarity and interoperability, in particular by creating a European network of services responsible for combating foreign digital interference (**SO13**). It will develop a **capacity-building assistance strategy**, aligned with critical democratic deadlines, in support of the most exposed States (**SO14**). In multilateral forums – **EU, G7, NATO, OECD, UN, French-speaking community, standardisation and hybrid bodies** – France will promote a democratic doctrine of response to manipulation and work to consolidate alliances (**SO15**).

In short, this strategy aims to make France a resilient democracy in the face of contemporary information threats. It is based on mobilising the population, coordinated interministerial engagement, close cooperation with regional, educational, industrial and scientific actors, and active engagement in European and international forums. Through this policy, France intends to equip itself with the necessary means to defend and enrich its democracy as a whole.

OVERVIEW

**COUNTERING
INFORMATION
MANIPULATION**

In a democracy, access to reliable, independent, and pluralistic information is essential. Today, in the age of digital platforms, the possibilities for producing, disseminating, and expressing information have reached a unprecedented level in human history. While these new features offered by technology have been presented as a renewal of our public debate, they have paradoxically brought with them a risk of manipulation induced by the operation of algorithms designed by a few dominant non-European players, as well as a threat of foreign digital interference linked to the malicious exploitation of these same features. As a result, the integrity of our online public debate has been structurally weakened, jeopardizing the expression of some of our freedoms.

In light of this worrying observation, a national strategy to combat the manipulation of information cannot and must not claim to regulate all aspects of content circulation. Its purpose is not to monitor, control, or standardize the plurality of expressions that constitute democratic debate. All public action in this area must comply with constitutional principles, fundamental rights, proportionality requirements, and freedoms of expression, communication and opinion.

Therefore, this strategy focuses primarily on intentional and coordinated actions to manipulate information by foreign actors, in particular foreign digital interference, the digital aspect of information manipulation, which is part of malicious hybrid strategies. From this perspective, public action focuses on inauthentic behaviour and dissemination channels (opacity, coordination, artificial amplification, monetisation) rather than on the content itself. It aims to preserve the conditions for free and open public debate within a secure, pluralistic, and transparent information environment.

In the face of these threats, it is up to the State to act. Not to regulate the content of opinions or to judge the legitimacy of expression, but rather to safeguard the very conditions of a sovereign public sphere, where information, ideas and opinions circulate freely. The objective is clear: to defend citizens' ability to form an independent view, to take part in democratic debate, and to make informed choices within a safe, pluralistic and transparent information environment.

In this spirit, this strategy is not based on a normative or prescriptive conception of discourse. Its purpose is to strengthen the foundations of our democracy by addressing deliberate information manipulation, not the content of opinions: the freedom to inform and to be informed, the transparency of the public sphere, and trust between citizens and institutions. Any action envisaged in this context will be carried out in strict compliance with the applicable national, European and international regulatory framework.

FRANCE, A PIONEER IN THE RESPONSE TO INFORMATION MANIPULATION

Convinced of the need to act, France has made the fight against information manipulation a national priority. In 2018, the public authorities took initial measures to combat information manipulation by setting up an interministerial coordination network, under the aegis of the SGDSN, designed to better understand this new threat. At the same time, the legislative framework was strengthened by the adoption of Law No. 2018-1202 of 22 December 2018 on combating the manipulation of information, which granted the Audiovisual and Digital Communication Regulatory Authority (ARCOM) and the interim relief judge new powers in this area.

Since then, France has developed structural assets: a doctrine, interministerial capacity, a stable legal framework and recognised operational expertise. The creation of VIGINUM in 2021 within the SGDSN has made it possible to structure this capacity and strengthen France's credibility in international cooperation.

This vision has been consolidated as the State has faced a digital landscape marked by these threats. This resolution has enabled France to develop a strong culture and operational capabilities that enable it to protect its interests.

Awareness has now spread throughout the entire ecosystem: governments, international organisations, private actors and civil society have stepped up their initiatives. France is playing an active role in these dynamics, particularly in European and multilateral forums.

In the information sphere, France has chosen to operate across three distinct areas: influence, information warfare, and the fight against information manipulation, the only area directly addressed by this strategy.

INFLUENCE

Influence is the result of an explicit, open and deliberate proactive strategy aimed at shaping foreign perceptions in order to create an environment favourable to national interests. Elevated to the status of a strategic function by the NATIONAL STRATEGIC REVIEW, it is now essential to the projection of our power and to our ability to counter competitors across the full spectrum of hybrid threats.

This approach encompasses both traditional diplomatic communication and emerging challenges relating to response, influence and the management of information threats, whether authentic or inauthentic in origin.

A specific governance structure for influence in the information field has been set up under the direction of the Ministry for Europe and Foreign Affairs. The aim of this system is to devise and implement influence operations targeting our strategic competitors.

INFORMATION WARFARE AND INFLUENCE-BASED CYBER OPERATIONS

Information warfare is directly involved in influence operations. It responds to a logic of power relations and aims to gain the upper hand over designated opponents in order to produce previously identified effects.

In the digital field, cyber influence operations (LII) form part of military operations conducted in the information environment. Placed under the responsibility of the Chief of the Defence Staff, overseen by the Ministry of the Armed Forces and led by COMCYBER, it acts on perceptions and behaviours to detect and counter attacks specifically targeting our armed forces or military interests.

LII is part of both the permanent posture of influence and cyber defence. Conducted exclusively outside national territory, it can be carried out autonomously or in a coordinated manner. It thus contributes to

strategic communication and analysis of the military operations environment in line with the armed forces' strategy.

THE FIGHT AGAINST INFORMATION MANIPULATION

A FIGHT WAGED AT THE INTERMINISTERIAL LEVEL

At the end of 2020, the assassination of Samuel Paty marked a turning point in the perception of the threat, revealing the dangerous nature of digitally amplified hate dynamics. This shock led, at the request of the President of the Republic, to the creation of the interministerial 'Honfleur' task force, whose work laid the foundations for a sustainable response mechanism.

This political will was formalised by the decree of 13 July 2021 creating, within the General Secretariat for Defence and National Security (SGDSN), the Vigilance and Protection Service against foreign digital interference (VIGINUM). This shift from a crisis management approach to a permanent structure now places the protection of French-language public debate at the heart of national defence and security.

A central component of the national strategy, VIGINUM detects and characterises foreign digital interference operations that could undermine the fundamental interests of the Nation. Under the authority of the Prime Minister, the SGDSN provides strategic coordination for this fight. In conjunction with the relevant ministries, it is responsible for identifying interference operations and coordinating interministerial protection and response actions.

A STRUGGLE CENTRED ON THE CONCEPT OF FOREIGN DIGITAL INTERFERENCE

The decree of 13 July 2021 formalised the concept of foreign digital interference (FDI) as *"an operation involving, directly or indirectly, a foreign actor (state or non-state), and aimed at the artificial or automated, massive and deliberate dissemination of allegations or imputations of facts that are manifestly inaccurate or misleading, and liable to undermine the fundamental interests of the Nation"*.

This text establishes a rigorous typology of the threat, based on four cumulative criteria: a potential harm to the fundamental interests of the Nation; an allegation or imputation of fact that is manifestly inaccurate or misleading; artificial or automated, massive and deliberate dissemination, or an intention to disseminate in such a manner; and the direct or indirect involvement of a foreign actor (state, para-state or non-state).

THE EUROPEAN AND INTERNATIONAL TERMINOLOGICAL FRAMEWORK

The French concept of FDI is part of an international framework structured around the concept of **FIMI** (Foreign Information Manipulation and Interference).

- **The European Union (EEAS)** defines FIMI as intentional and coordinated activities, carried out by state or non-state actors, which have a negative impact on political values and processes. This definition is used within the G7 (RRM).
- **NATO** uses a "FIMI toolbox" to describe manipulative activities targeting the Alliance and its Allies, including disinformation and information operations.
- **The OECD** targets coordinated efforts on behalf of a foreign power to corrupt decision-making and public discourse.

The fight against information manipulation is part of a legal framework that has gradually evolved under the influence of new technologies, but whose unchanged objective remains to reconcile freedom of expression, protection of individual rights and public order, and the pursuit of the general interest.

- **The cornerstone remains the 1881 Law on the Freedom of the Press**, which reflects the balance between freedom of expression and responsibility enshrined in Article 11 of the 1789 Declaration of the Rights of Man and of the Citizen. While reaffirming the principle of freedom of expression, stating in Article 1 that "Printing and bookselling shall be free", the law also penalises its abuses, including where these arise from public expression (as opposed to publication through the press) and stem from the dissemination of "false news". Article 27 thus specifically sanctions the publication or reproduction of false news where it is made in bad faith and disturbs, or is likely to disturb, public order.

The law also penalises other abuses of freedom of expression that are not directly linked to the truthfulness of the statement concerned, notably defamation and insult (defined in Article 29 and punished respectively under Articles 32 and 33).

- **The 1986 Law on Freedom of Communication** adapted the obligations applicable to press undertakings to the specific characteristics of audiovisual communication. While reaffirming that communication is free (Article 1), it lays down various obligations for audiovisual media, notably aimed at safeguarding fair political debate, and establishes a regulator empowered to sanction breaches: ARCOM.

This framework, designed before the digital age, remains the regulatory benchmark, the main principles of which have remained unchanged. It has been supplemented by tools adapted to the current technological environment:

- **the law of 22 December 2018 established the first legal definition of information manipulation in an electoral context**, targeting allegations or imputations of fact that are manifestly inaccurate or misleading and disseminated deliberately, artificially or automatically and on a massive scale in order to undermine the integrity of an election (Art. L. 163-2 of the French Electoral Code). This initiative complements a pre-existing system of election protection: with a view to ensuring the integrity of democratic debate, Article L. 97 of the French Electoral Code punishes fraudulent practices, such as the dissemination of false news or slander, with the aim of diverting votes or encouraging voter abstention;
- **the European Digital Services Act (DSA)**, fully applicable since 2024, which makes platforms accountable by requiring them to mitigate "systemic risks" to civic discourse and public safety (Art. 34). It is supplemented by the **Code of Practice on Disinformation**, which binds signatories (platforms, advertisers, civil society) to specific commitments regarding transparency in advertising funding, combating inauthentic accounts and providing researchers with access to platform data.

Beyond the texts dedicated to digital technology and elections, French law also includes a set of cross-cutting laws that act as barriers against these foreign manoeuvres:

- **at the national level (social cohesion)**: laws against racism, anti-Semitism and online hate speech (1972, 1990, 2021) are essential. Interference strategies systematically exploit our identity divisions in order to polarise opinion. By sanctioning such discourse, French law reduces the ability of foreign actors to turn our internal debates into instruments of destabilisation.
- **at European level (media freedom)**: the European Media Freedom Act (EMFA) of 2024 follows the same logic of resilience. By protecting editorial independence and preventing platforms from arbitrarily removing journalistic content, it guarantees citizens' access to reliable information, which is an element of resilience in the face of information manipulation.

THE CHANGING INFORMATION LANDSCAPE: THE INCREASING DIGITISATION OF OUR PUBLIC DEBATE

FROM THE EDITORIAL MODEL TO DIGITAL PLATFORMS

The emergence of traditional media, whether audiovisual or print, has been accompanied by a stable set of national regulations comprising our constitutional framework, the electoral code, the 1881 law on freedom of the press and the 1986 law on audiovisual communication. These rules are designed to ensure a balance between freedom of expression, the regulation of public media and the preservation of the public interest. This framework has been designed for identifiable actors, structured editorial chains and clearly established responsibilities.

Since then, our information environment has been disrupted by the digitisation and algorithmisation of communication channels. The now widespread ability to produce, transform and disseminate content on a large scale has lowered the technical and economic barriers to accessing the digital public space, changing the dynamics of information circulation.

In the pursuit of structuring the traditional media ecosystem, the production, dissemination and monetisation of information by digital services are increasingly part of a framework in which advertising, subscriptions and attention capture determine the viability of the media. These models rely heavily on automated recommendation and targeting mechanisms specific to the platform economy. They often favour virality over reliability and editorial prioritisation, and can propel certain content without sufficient consideration for its source or veracity.

The immediacy of reactions enabled by this model, combined with the fundamental importance of freedom of expression in a democracy, has shifted a growing part of public debate to social media networks, most of which are operated by companies based outside the national and European territory and subject to their own economic, or even ideological, logic. At the same time, there has been a steady erosion of the economic viability and investigative capacity of traditional media.

This evolution in the ways in which information is consumed poses a systemic risk to the sincerity of public debate: a small number of private actors now govern the core of our conversational infrastructure according to logic that may, in some respects, fuel democratic debate, but is fundamentally external to its purpose.

In this context, manipulative actions are no longer aimed solely at persuading, but also at saturating attention, shifting frames of reference, undermining common points of reference, sowing confusion and disrupting the conditions for calm public debate.

A PUBLIC DEBATE UNDER THREE PRESSURES

In this context of profound changes in the information landscape, **our digital public debate is exposed to a growing number of vulnerabilities**, under the influence of three distinct pressures: strategic, systemic and narrative.

STRATEGIC PRESSURE: INTERFERENCE AS A TOOL OF POWER

First, our information space is under increasing strategic pressure, in the context of a deteriorating international environment that is facilitating the emergence of global digital conflict.

Characterised by the free flow of ideas and open access to broadcasting platforms, this space has thus become the preferred arena for hybrid confrontations, where several foreign state competitors have made information manipulation a strategic tool in its own right, linked to their diplomatic, economic or security objectives. Indeed, foreign actors are taking advantage of this context to attempt to interfere in our public debate, alter collective perception and influence decision-making processes.

These strategies aim to sow confusion, polarise society and, ultimately, erode public confidence in democratic institutions and the media. This trend is particularly marked by the persistence and growing sophistication of foreign information operations, which deploy complex mechanisms enabling them to carry out long-term planned actions, but also to act opportunistically in response to current events. In this regard, the *RRN/Doppelgänger* information operation impersonates legitimate media outlets in order to reinforce the perceived credibility of its messages and undermine trust in information. It is also characterised by overt and uninhibited information strategies on the part of foreign competitors, who coordinate their use of a range of digital levers in the service of offensive public diplomacy aimed directly at civil societies. In particular, the digital public debate surrounding ongoing conflicts (notably in Ukraine and between Israel and Hamas) is regularly exploited by threat actors to accentuate divisions within Western societies.

For example, Russia's main objective is to undermine Western support for the war in Ukraine, while destabilising European countries (including France), particularly during election periods. This objective is especially embodied by the network known as *Storm-1516*¹, active since August 2023 and very likely operated by a Russian intelligence service. Having carried out more than 150 information operations in two years, *Storm-1516*'s main characteristics are the coordinated production and dissemination of false audiovisual content, sometimes modified by artificial intelligence, aimed at damaging the image of its targets, including France.

Drawing on a structured doctrine and dedicated resources, the information strategy of the People's Republic of China is primarily aimed at promoting Beijing's image among foreign audiences. To this end, pro-Chinese Communist Party actors led a campaign targeting Dassault Aviation's Rafale fighter jet during the recent conflict between India and Pakistan. It relied on the dissemination of false content, the use of fake accounts and a coordinated amplification of online interactions in order to damage the reputation of this export weapons system.

In the summer of 2023, in the context of the conflict with Armenia in Nagorno-Karabakh, Azerbaijan deployed an aggressive strategy of interference against France's sovereignty in its overseas territories and Corsica, by amplifying independence movements and ideas. These manoeuvres were supported by a group specially created for this purpose, the BAKU INITIATIVE GROUP (BIG), as well as by inauthentic digital activity targeting New Caledonia in particular, notably through the use of fake accounts, the creation of

¹ *Storm-1516* refers to an information modus operandi (IMO) attributed to Russian actors, active since at least August 2023, comprising several dozen coordinated digital information operations aimed at disseminating false or misleading narratives to Western audiences, in particular to discredit governments (Ukraine, European states) or to target electoral processes and political figures.

misleading visuals and the artificial amplification of this content.

European democracies face a major challenge: protecting open public debate that respects everyone's freedom of expression. This openness is exploited by hostile actors. The challenge is to protect our fellow citizens from attempts to manipulate information by strengthening our capacity for detection and response, including attribution where possible, while continuing to build our societal resilience through collective mobilisation.

SYSTEMIC PRESSURE: PLATFORMS, THE ATTENTION ECONOMY AND AI

Furthermore, our digital information space is subject to increased systemic pressure, exerted by changes in the digital landscape itself. This systemic pressure is the result of two joint transformations: the reconfiguration of information circuits around platforms and the rapid integration of AI into content production and distribution.

On the one hand, the evolution of the information landscape itself, which is seeing the emergence of a new digital information ecosystem, characterised by the dominant role of social networks, some of which are now openly used by their executive officers for political purposes, the growing role of influencers, and the expansion of alternative opinion media. These developments are contributing to a further erosion in the consumption of traditional media and tend to blur the distinction between factual information and opinion. In particular, a large number of inauthentic news websites, run by foreign digital communications companies linked to Chinese or Russian interests, publish articles *en masse*, translated into French using artificial intelligence, and attempt to position themselves in the French digital landscape by presenting themselves as official French media outlets.

On the other hand, the rise of artificial intelligence is radically redefining digital usage. It is leading to a profound restructuring of the attention economy, and more specifically, of the way information is produced, distributed, consumed and monetised. AI thus acts as an accelerator for a profound transformation of power and value in the digital landscape: competition between large platforms, which are attempting to maintain their competitive advantage by becoming “gateways” to AI; the emergence of new players and economic models; impact on traditional publishers, forced to adapt in an environment where their visibility and traditional distribution channels are being challenged. For example, the Russian company Social Design Agency, which carries out some of the pro-Kremlin interference operations, uses AI mainly to disseminate content and protect its bots.

Furthermore, by facilitating the creation and large-scale dissemination of hyper-realistic synthetic content – whether images, videos, sounds or text – the proliferation of AI thus raises legitimate fears of a structural increase in the level of threat linked to foreign digital interference, both in terms of new vectors and new vulnerabilities. Beyond this, specific attention must be paid to the use of AI for the purpose of amplifying hidden algorithmic biases, as well as to the possibility that AI models themselves may be altered during their construction phase by information manipulation operations.

NARRATIVE PRESSURE: EXPLOITATION OF POLARISING ISSUES

Finally, our information space is subject to uninhibited narrative pressure, marked by the weaponisation of powerful themes, such as freedom of expression.

An absolutist view of freedom of expression, as conceived by certain conservative movements in the United States, is deliberately being introduced into the European public debate.² This issue is also being opportunistically exploited by online platforms, perpetuating a misleading, even erroneous, conception

² The US National Security Strategy explicitly states the following position: “American diplomacy should continue to stand up for genuine democracy, freedom of expression, and unapologetic celebrations of European nations’ individual character and history. America encourages its political allies in Europe to promote this revival of spirit, and the growing influence of patriotic European parties indeed gives cause for great optimism” (U.S. National Security Strategy, November 2025, p. 26).

of the objectives of European digital regulation (DSA).

In addition, the dismantling of the US development aid and civil society support system marks a major break with the past, destabilising a long-established system of support for information integrity.

While in the 2010s these dynamics were concentrated around election periods, they now extend to all areas of public debate. They aim to polarise opinion, undermine social cohesion, erode trust in traditional media and break the link between citizens and institutions – to the point of causing public disorder.

Particular attention must also be paid to overseas territories, which have specific vulnerabilities in the information sphere. Due to their geographical location and history, these territories may be subject to targeted information campaigns. Beyond detection, the response requires a capacity for local engagement: institutional partners, local media, and educational and community stakeholders, in order to limit the spread of hostile narratives and strengthen trust in mediating channels (media, expertise and institutions).

ADDRESSING THE VULNERABILITIES OF PUBLIC DEBATE

WHY DO THESE TACTICS FIND FERTILE GROUND?

The effectiveness of information manipulation operations stems less from the intrinsic power of the messages than from their ability to exploit pre-existing vulnerabilities in the target societies. They stem both from a structural vulnerability specific to open democracies and from endogenous, social and cultural vulnerabilities.

Democracies are based on principles – freedom of expression, pluralism, transparency, the rule of law – **which underpin their legitimacy but can be exploited asymmetrically.** Hostile actors can act quickly, at limited cost and below the threshold of illegality, where public authorities are bound by requirements of proportionality, procedural guarantees and democratic control.

These operations also exploit social, economic, cultural and civic weaknesses. They build on existing divisions to transform the nature of public debate, polarise exchanges and weaken the mediating role played by the media, experts and institutions. Periods of crisis or political tension tend to amplify these dynamics, simultaneously reinforcing inequalities and mistrust.

Several types of vulnerabilities thus structure the information environment. Susceptibility to manipulative narratives is heightened in contexts of precariousness, exclusion and weakened social ties. The economic fragility of the media and the concentration of visibility on a limited number of intermediaries weaken information mediation and shared reference points. The rise of artificial intelligence accentuates these vulnerabilities through the mass production of synthetic content and the increasing opacity of algorithm-based recommendation mechanisms.

Distrust of institutions is a risk multiplier: when public discourse is systematically challenged, the information space becomes more receptive to polarising narratives and destabilisation efforts.

These vulnerabilities also affect the response capabilities of actors engaged in defending public debate – institutions, media, civil society, educational and economic actors – whose actions take place in an increasingly constrained and fragmented environment.

Finally, the perceived ambiguity of the State's role in the information space can itself become a factor of vulnerability. When its aims, limits and guarantees are not clearly identified, public action can fuel the mistrust it seeks to contain.

HOW CAN WE ASSESS THE EFFECTS OF THESE MANOEUVRES?

The effects of information manipulation operations are difficult to measure accurately. They result from complex interactions between exposure to content, recommendation mechanisms, social structures and the political context. The available indicators (reach, engagement, virality) do not fully describe the real impact on collective representations, behaviours and decisions. These operations do not generally act as a single cause, but as a factor amplifying already existing tensions.

The uncertainty surrounding measurement does not mean there is no impact. These operations rarely seek to convert audiences on a large scale; rather, they aim to produce diffuse and cumulative effects: increasing information noise, saturating attention, instilling doubt, weakening trust in the media, expertise and institutions, and driving polarisation through the selective amplification of controversies. In this way, they can gradually degrade the conditions for public debate based on shared reference points, without any clearly identifiable triggering event.

One thing remains clear: if these operations are repeated, industrialised and continuously adapted, it is because they are effective. Hostile actors invest in interference and automation mechanisms, measure reactions, adjust their narratives and reuse their methods. For them, information manipulation is a low-

cost, flexible lever that can be exploited in open environments.

Public action is therefore based on a risk management approach. It must reduce established vulnerabilities, even where the precise impact of a campaign cannot be demonstrated retrospectively. Demanding exhaustive proof before acting would create a lasting imbalance that would benefit adversaries.

This risk management approach requires a precise definition of the scope of public intervention.

A TARGETED SCOPE OF PUBLIC ACTION

The national system for combating information manipulation is based on a clear democratic principle: it has neither the purpose nor the mandate to qualify national dynamics. Its scope of intervention focuses on the detection of technical manipulation and coordinated operations involving a foreign origin, in the interests of national security.

This approach – based on democratic guarantees and objective technical criteria – focuses resources on artificial amplification, automation and inauthentic coordination. It protects internal pluralism by separating the analysis of manipulation processes from any assessment of opinions, actors or movements.

PROJECTIONS FOR 2030

Looking ahead to 2030 is necessary, but uncertain. Technological, economic and informational transformations no longer progress in stages: they are accelerating and combining with effects that are difficult to anticipate. They no longer concern only new tools or uses: they are profoundly changing the way information is produced, disseminated and received by the public, and with it, the ways in which opinions are formed and collective debate takes place.

This is not a sudden upheaval or an extreme scenario. Several of these dynamics are already visible, while others are a continuation of established trends. The challenge in the coming years will lie less in their emergence than in their widespread adoption and lasting integration into the everyday use of digital services.

Information manipulation operations involving foreign actors are likely to evolve in this new environment. Three technical dynamics, already observable, are shaping this evolution in the dominant scenarios at this stage:

- the ability to produce content on a very large scale, often at low cost;
- the increasing automation of its dissemination and interaction;
- and the centrality of selection and recommendation systems, whose transparency is subject to increasing regulatory requirements, with effects that are still unevenly measured.

THE TRIVIALISATION OF SYNTHETIC GENERATION: RISK OF A POSSIBLE WEAKENING OF EVIDENCE

For several years now, artificially generated content – text, images, sound or video – **has been circulating widely online.** By 2030, this production could become entirely commonplace, integrated into everyday tools and ordinary communication and information-seeking activities.

The novelty lies not only in the volume of content produced, but also in its cumulative effects on trust. When digital traces can be produced instantly and in large numbers, their probative value tends to weaken. What previously served as evidence as an isolated visual or audio element becomes more fragile and more easily contestable. However, technical mechanisms for certifying, tracing and signing content are emerging in parallel (e.g. watermarking), although there is no guarantee at this stage that they will become widespread.

In this context, the boundary between information, commentary, interpretation and manipulation becomes less clear. When combined with coordinated dissemination capabilities, this development potentially increases the effectiveness of foreign information manipulation operations based on the widespread and deliberate dissemination of misleading content, by reducing the public's ability to distinguish between authentic and fabricated content.

ALGORITHMIC HYPER-PERSONALISATION: TOWARDS AN INCREASINGLY FRAGMENTED REALITY

This normalisation is accompanied by greater personalisation of information. Selection and recommendation systems could evolve towards increasingly individualised differentiation, incorporating preferences and behaviours across certain categories of use and platforms.

Polarisation would then no longer result solely from differences of opinion, but from the fact that individuals no longer have access to the same topics or narratives, with different perspectives. This fragmentation creates fertile ground for interference strategies, which can target segmented audiences, tailor messages and exploit existing divisions.

AUTOMATION OF INTERACTIONS: PUBLIC DEBATE CONSTRAINED BY ATTENTION

The automation of interactions has already crossed a threshold. Devices, such as AI agents or agentic models, capable of producing, relaying and amplifying statements are beginning to participate in online exchanges in certain environments. As they become more fluid and autonomous, they may become commonplace in certain segments of platforms, without always being identifiable as such despite the development of automated detection and labelling tools.

The challenge is no longer just to convince, but to impose a dynamic of attention: capturing attention, keeping a topic in the foreground and, ultimately, saturating the capacity for exchange. Public debate may thus be structured less by the quality of the arguments than by the ability to direct or disperse collective attention. These approaches are consistent with modes of interference based on the artificial and coordinated dissemination of content, aimed less at direct persuasion than at the lasting disruption of public debate.

NEW DIGITAL INTERMEDIARIES: A POSSIBLE TRANSFORMATION OF ACCESS TO INFORMATION

Access to information is expanding to new intermediaries: conversational interfaces, services integrated into everyday tools, systems capable of formulating direct responses. These devices no longer simply refer to sources: they select, reformulate and prioritise content.

Vulnerability therefore no longer lies solely in the production of information, but in the criteria for selection and presentation, which partly determine perceived credibility. Often invisible, these mechanisms influence the understanding and prioritisation of topics, according to architectures and parameters that vary depending on the service, without always being explicit. They can thus be targets for foreign information operations seeking to indirectly influence opinion formation.

NEW MODES OF INFORMATION CONSUMPTION: STRATEGIES INCREASINGLY ADAPTED TO AI

As artificial intelligence becomes an interface for accessing information – generative engines, conversational assistants, synthesis tools – information interference strategies are likely to evolve. They may no longer target only audiences, but also the systems responsible for producing, organising and reformulating information.

In an environment where informational value increasingly relies on data – training corpora, indexed content, model adjustment signals – interference can be carried out upstream, through direct or indirect intervention on these data sets, more easily on the indexing and search layers in open environments than on the fundamental models themselves, whose training corpora should, in theory, be more filtered and prepared. This dependency increases the sensitivity of smaller linguistic ecosystems. The French-speaking digital space, which is less dense than the English-speaking space, may therefore be particularly vulnerable to imbalances or targeted alterations of corpora.

These approaches correspond to adverse modes of operation: intentional, tool-based, automatable action that is compatible with large-scale interventions. They can take the form of injections of targeted content into spaces heavily explored by automated systems, optimisations for generative engines (techniques similar to SEO adapted to AI systems), or alterations to reference datasets when they are open, contributory or insufficiently controlled. The objective is no longer just the visibility of a message, but its probability of being integrated into automatic summaries or implicit credibility rankings.

These strategies offer their promoters several advantages: limited cost, difficult attribution, delayed effects, and the ability to operate below the usual detection thresholds. They are long-term strategies that aim for structural effects rather than one-off impacts.

THREE GUIDING PRINCIPLES FOR PUBLIC ACTION

In order to fully comply with the requirements set out above, this national strategy to combat information manipulation is based on three fundamental principles: openness, networking and integration. These principles aim to coordinate institutional responses, broaden the scope of actors involved and strengthen the resilience of society as a whole in the face of information threats, in strict compliance with constitutional, European, and international democratic principles.

OPENNESS

Unlike other areas of national security based on confidentiality, the fight against information manipulation relies to a large extent on publicly available methods and resources. This approach marks a significant paradigm shift: it prioritises transparency, verifiability and the mobilisation of all stakeholders.

VIGINUM's work illustrates this approach. The service bases its activity on publicly available data, publishes its analyses and makes some of its methods and tools accessible. This strategic choice, which will be strengthened and made systematic, aims to enable reproduction, verification, challenge and contribution by third parties. It is not without its drawbacks – notably the risk of inadvertently promoting threats or exposing national capabilities – but it is applied judiciously, on a case-by-case basis.

This logic of openness and transparency is a lever for democratic reinforcement: by giving the public the means to understand the mechanisms of manipulation, it reduces their effectiveness. An information manipulation campaign cannot operate sustainably without opacity. Transparency thus becomes both a preventive and a curative tool, contributing to a better understanding by citizens of the issues related to foreign digital interference.

NETWORKING

The fight against information manipulation cannot be carried out by a single entity. It relies on distributed mobilisation, based on cooperation between administrations, institutions, technical actors, regulators, researchers, the media, platforms, civil society and citizens – each at their own level of responsibility.

This cooperation can take several forms, as detailed in this strategy: information exchanges, joint actions, and the establishment of permanent or ad hoc mechanisms. Several national bodies illustrate this dynamic. Other forms of coordination exist at bilateral, sectoral or European level, such as the Network of Digital Regulators, the European Digital Services Committee and the European Rapid Alert System.

Within the State, this approach requires an interministerial approach: beyond the services specialising in detection or response, it must be possible to mobilise all administrations involved in the social, health, educational, cultural or civic fields. Citizen engagement, public relations and media literacy must therefore be part of this collective dynamic.

INTEGRATION

Finally, the fight against information manipulation requires a comprehensive and systemic approach. In an interconnected digital environment, no area of social life is immune to the circulation of content. Traditional boundaries – between the physical and the virtual, the national and the international, the public and the private – are tending to disappear in favour of cross-cutting phenomena involving a diversity of actors.

The response must be commensurate with this complexity: it requires increased coordination between institutions, mutual recognition of skills and the ability to mobilise all stakeholders – administrations,

businesses, research laboratories, associations and citizens.

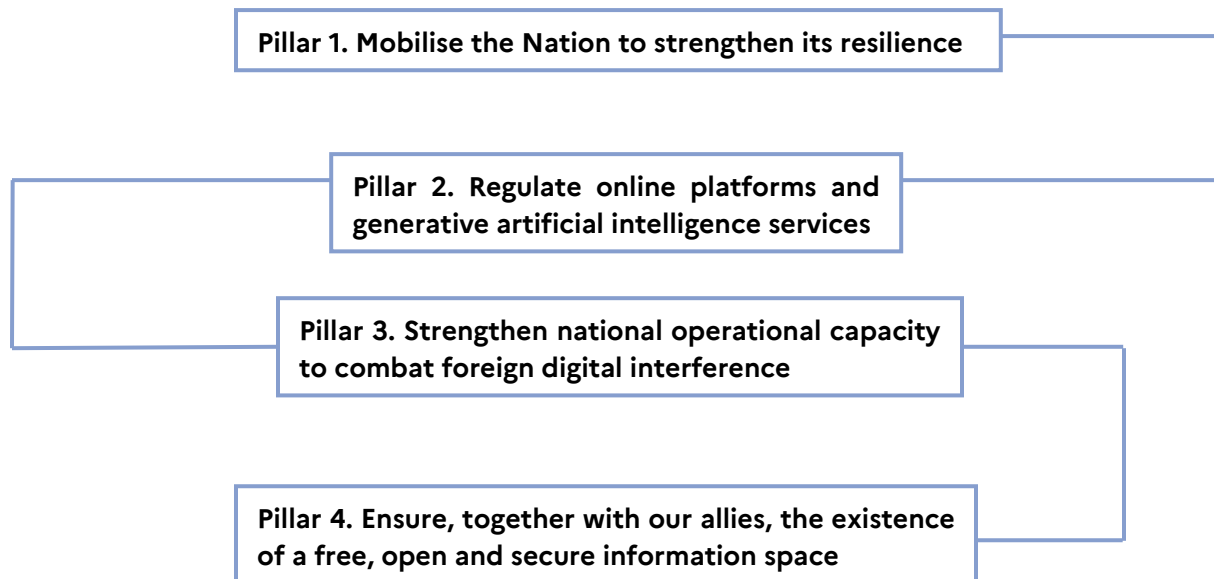
Integration also refers to the need to share information, while respecting security requirements. Strengthening mutual trust between public and private actors relies on the controlled circulation of what is known, what is being assessed, and what remains uncertain.

Through this approach, every entity and every citizen can become an actor in informational resilience by participating in the detection, understanding, or remediation of attempts at manipulation.

These three principles – openness, networking and integration – form the operational foundations of this strategy. They should enable us to capitalise on the dynamics already in place, while ensuring collective momentum and operationalisation capable of responding to the growing intensity of the challenges involved in combating foreign interference. They will guide action in the years to come, including in the face of as yet unidentified threats, in a constantly changing information environment, and will serve as a basis for the strategic objectives defined later in this document.

A STRATEGY BROKEN DOWN INTO 15 STRATEGIC OBJECTIVES

In line with the National Strategic Review and as an extension of the State's action to combat information manipulation, this strategy adopts a structured approach based on four main pillars:



Broken down into 15 strategic objectives, this comprehensive, coordinated and evolving strategy aims to consolidate France's lead in preserving the integrity of public debate and to continue its efforts to build democratic resilience in the face of information manipulation. It favours strategic coherence over exhaustiveness, in order to focus public action on the most effective and mobilisable levers.

Rather than seeking illusory completeness through an exhaustive inventory of actions, the strategy proposes concrete courses of action, shared guidelines and non-limitative operational objectives designed to guide public action in the short and medium term. Its ambition is to imbue the approaches of the actors involved, whether state or non-state, with a clear, shared and evolving philosophy of action.

Given the scale of the threat, the central challenge identified by the strategy is to establish and lead a collective at the national level and beyond, with a view to a concerted response at the international level. This involves:

- **involving the entire population** in understanding manipulation phenomena;
- **widely sharing information useful** for the prevention and detection of these phenomena;
- **strengthening the capacity for action** of public entities and actors in the field;
- **pooling available operational resources** to ensure a coordinated and effective response.

At the heart of this strategy lies the ambition to move beyond the mere fight against information manipulation and to build a society capable of sustaining trust and shared reference points. Every citizen, public authority and private actor must have the means to access information in an informed way, to understand the mechanisms of interference, and to contribute actively to democratic debate. This ambition is supported by other levers – digital services, education, culture and regional development – which, although outside the strict scope addressed here, help to strengthen and sustain that trust.

Mobilise the Nation to strengthen its resilience

Building a resilient society by empowering every citizen to become an informed actor against information manipulation, through a unique engagement programme and a network uniting citizens, institutions and key civil society actors.

PILLAR

01

In the face of information manipulation and foreign digital interference, a key strategic challenge is to **strengthen the resilience of society** as a whole by addressing the **cognitive, social, educational and cultural factors** that such manipulation exploits.

This requires building a **shared foundation of critical skills and knowledge** accessible to all, covering the methods and techniques used by foreign actors to interfere in our digital debate, as well as the specific risks posed by the use of certain digital technologies (generative AI, recommendation algorithms, etc.); creating **pathways for engagement and specialisation** around information-related issues; and mobilising **educational, community, scientific and civic levers** across the entire country.

The first condition for this resilience is the establishment of a national capacity for expertise, capable of detecting, characterising and understanding information manipulation operations (SO1). To this end, France is promoting a federative approach centred on an Academy for Countering Information Manipulation, based within the VIGINUM service. Organised in a distributed manner, this structure will draw on existing actors to form a network of experts, provide key skills, transfer technical resources and encourage the emergence of regional representatives. This network will form the operational backbone of France's democratic resilience strategy.

At the same time, the national strategy aims to roll out a comprehensive training, awareness-raising and research programme, backed by schools, higher education and the academic world **(SO2).** This programme will gradually integrate the issues of information manipulation into school curricula, offer training modules for teachers and researchers, and support high-impact interdisciplinary research projects. The aim is to **build a sustainable knowledge ecosystem** capable of informing public action and strengthening critical thinking from an early age.

Beyond the education system, the State will also mobilise civic engagement mechanisms to train young people to actively defend public debate (SO3). The Defence and Citizenship Day (JDC), the Voluntary Military Service, as well as the Civic Service and Civic Reserve, will all provide opportunities to disseminate content relating to the fight against information manipulation. The digital civic reserve will be mobilised to train and support individuals wishing to take action in the fight against information manipulation. Dedicated educational modules and initiatives will be introduced to boost engagement and open **pathways into the civic reserve.**

Finally, the strategy relies on the widespread dissemination of a civic culture of protection against information manipulation (SO4). This approach is based on flexible and participatory formats (workshops, debates, forums), supported locally by a **network of trained individuals** from the fields of media and information literacy, popular education, associations and the Academy for Countering Information Manipulation.

Popular or state initiatives which are already established nationally could serve as a basis for structuring public forums for discussion on information manipulation. The objective is to **create a collective culture among the entire population,** based on proximity, openness and prevention.

STRATEGIC OBJECTIVE 1. BUILDING A COLLECTIVE CAPACITY TO COMBAT INFORMATION MANIPULATION

Building a collective capacity to combat information manipulation requires to train actors who are able to mobilise their knowledge in an integrated manner within the professional and social structures that are directly or indirectly involved in the functioning of our information environment.

A first requirement is to ensure the reliability of the national information environment in the broadest sense, whether digital or not. To this end, it is important to share the necessary elements of understanding and analysis, whether they come from research, civil society or the State, as a priority with those who have a particular role in the functioning of our common information space.

Over the long term, this knowledge, expertise and practices must be integrated into all the structures that are critical to the functioning of the country. This requires organisational adaptations, as well as the emergence of a new generation of highly qualified professionals in fields such as strategic monitoring, social media analysis, the assessment of algorithmic manipulation, the malicious use of AI systems, technical response mechanisms, digital investigation, and the technical understanding of information dynamics.

Although this expertise is crucial, it is not currently structured on a large scale at the national level. This field faces a shortage of skills, made worse by the social and gender under-representation that more broadly characterises the digital sector, as well as by a mismatch between the profiles being trained and the actual needs in the field. In this context, it is essential that France take action in both the short and long term.

In the short term, it is important to provide all local and national decision-makers, senior civil servants, media executives and journalists with clear information on the technical and technological mechanisms used in information manipulation operations. The professional training bodies specific to each professional group may be mobilised for this purpose.

This should enable a comprehensive understanding not only of specific events but also of global and structural mechanisms in a context where foreign interference is increasingly frequent and tangible.

This initial communication will be supplemented by the regular publication of information bulletins concerning the methods of foreign interference detected in the information sphere, together with general explanatory material similar to that already disseminated by VIGINUM.

In the long term, it is important to invest heavily in the development of these skills, in particular by integrating them into existing training courses in the fields of public services, media, social sciences and digital technology.

In partnership with local authorities, higher education institutions, academies, associations, the media, public training operators and relevant economic actors, the State will develop a structured national training policy aimed at key players.

This federative approach will make it possible to capitalise on existing resources while promoting the expertise acquired by a large number of actors, whether national, European or international. A link will also be established with cybersecurity training.

GIVE THE ACADEMY FOR COUNTERING INFORMATION MANIPULATION (LMI ACADEMY) A UNIFYING ROLE

By 2027, France will structure and roll out an Academy for Countering Information Manipulation (Académie de la LMI) within the VIGINUM. It will be responsible for publishing and disseminating the necessary bases of technical knowledge, most of which already exists, whether they relate to the technical aspects or the social, psychological or behavioural factors, digital or otherwise, involved in the manipulation of information. It will involve all relevant public stakeholders and existing training programmes.

This knowledge must above all focus on information manipulation techniques, as well as long-term structural dynamics, whether social, psychological or technological, and the factors that lead to the adoption of certain behaviours.

The Académie de la LMI will have three core functions:

- **to design and share educational resources** tailored to each target audience (education, awareness-raising, training), intended for elected officials, prefectures, local authorities, public administrations, the National Education System, the media, businesses, associations and the general public.
- **to train as many people as possible,** disseminating acquired skills and technological tools and ensuring the dissemination of a common operational culture to deal with foreign digital interference. This network will be linked to cybersecurity training initiatives, with a view to complementarity.
- **to develop an international capacity-building programme,** in line with our national and European priorities, aimed at foreign partners wishing to set up structures similar to VIGINUM. This cooperation will also enable the Academy to strengthen its own resources through the methodological and educational contributions of its partners.

STRATEGIC OBJECTIVE 2. BUILD AN EDUCATION AND RESEARCH SECTOR DEDICATED TO INFORMATION RESILIENCE

Establish a coherent, interdisciplinary approach to transgenerational education and transdisciplinary research in order to strengthen society's ability to understand, detect and counter information manipulation in the long term.

Faced with the scale and complexity of information manipulation, France is implementing a coherent, structured and interdisciplinary public policy on information education and research into information dynamics.

This strategy aims to build a comprehensive long-term approach, ranging from cross-generational public awareness to high-level academic research, by mobilising all relevant stakeholders on a long-term basis: schools, universities, research institutions, the media, the cultural sphere and civil society. The aim is to **spread, across all levels of society, the critical skills necessary** for understanding, detecting and addressing information manipulation, with a view to strengthening democratic resilience.

STRENGTHENING MEDIA AND INFORMATION LITERACY IN THE SCHOOL SYSTEM

Media and information literacy (MIL), one of whose objectives is to develop critical thinking in the processing of information, and the integration of educational elements on information manipulation into the relevant teaching programmes, particularly moral and civic education, are a fundamental lever for the education of young citizens. This integration, already in place in the new curricula gradually introduced since the start of the 2024 school year, will be further strengthened across the various teaching programmes.

Partnerships between the ministry responsible for national education and VIGINUM or ARCOM will contribute to the following objectives:

- **wider dissemination of the MAGISTÈRE self-training pathway and the rollout of academy-level training programmes to support it;**
- **strengthened distribution of existing resources**, in particular those produced by CLEMI and promoted on the *Éduscol* website;
- **the development of new resources:** materials for LUMNI ENSEIGNEMENT, in collaboration with INA and FRANCE TV, as well as tools such as the evolution of THE OSINT PROJECT and the PIX platform, whose educational uses will be promoted and expanded.

MOBILISING ACADEMIC PROVISION AND HIGHER EDUCATION STAKEHOLDERS

The relevant ministries, in particular those responsible for higher education, health, families, independence and disabled persons³, will be fully mobilised to remind operators of the importance of taking into account the fight against information manipulation and critical education on media and information when developing their training strategies. Several courses prepare students for careers in critical media and information literacy and journalism, as well as open source intelligence (OSINT) and information processing, and will be able to train experts specialising in these issues. They are based on the disciplines of information and communication sciences, law, digital and data sciences, cognitive sciences, and geopolitics – particularly in the digital field.

Awareness-raising activities may be offered to doctoral students as part of compulsory training in scientific integrity and to newly recruited teacher-researchers. Conversely, their skills can be mobilised in conjunction with those of society as a whole in a spirit of open research. These actions could draw on the awareness-raising and training initiatives already structured and developed within the network of university libraries and scientific information training providers, and could also draw on the network of

³ See National strategy to combat health misinformation

scientific information professionals and the platforms for disseminating scientific content supplied by higher education institutions.

The subject will also be included in methodology courses taught to undergraduate and master's students. An analysis will be carried out to assess the integration into existing courses of content dedicated to identifying the technical processes used to manipulate information, and support measures to reinforce the presence of these topics will be proposed to institutions. At the same time, a **network of communications professionals** within higher education and research institutions will be established to strengthen monitoring, information-sharing and response capabilities in the face of information manipulation.

This network will improve the accessibility and visibility of work and content that help shed light on current affairs, respond to information attacks, showcase research projects and findings, and contribute both to enriching public debate and to promoting scientific culture, attractiveness and the democratisation of science. It will build on, and coordinate in particular with, efforts to combat disinformation led by university libraries and documentation structures within higher education and research.

SUPPORTING INTERDISCIPLINARY RESEARCH ON INFORMATION PHENOMENA

The main challenge is to accurately identify research needs by establishing **a comprehensive overview of existing resources and gaps**, whether in institutional or academic spheres or in public or private research sectors. This assessment will enable **the most appropriate funding (dedicated programmes or chairs) to be mobilised** to support research, while guaranteeing both the freedom inherent in research and its contribution to understanding these major societal challenges.

As a first step, this will involve a **two-pronged approach**: on the one hand, conducting in-depth studies on the **reconfiguration of the online information economy** and, more broadly, the **information landscape** (business models, technical architectures, emerging technologies, value chains), incorporating the **major transformative potential** of generative AI; on the other hand, analysing the **impact of information manipulation**, in terms of exposure, reception and modification of attitudes and behaviours, as well as the **remedial measures** proposed.

STRATEGIC OBJECTIVE 3. MOBILISE CIVIC ENGAGEMENT PATHWAYS TO PROTECT PUBLIC DEBATE

Mobilise civic engagement mechanisms to raise awareness among younger citizens, promote the skills they have acquired and build a pool of active citizens who can counteract the manipulation of information.

Civic engagement is a strategic lever for raising awareness, training and mobilising a generation of citizens who are actively involved in protecting public debate. To foster a society that is resilient to information manipulation, the State will strengthen and adapt **existing engagement mechanisms** by fully integrating issues related to foreign digital interference.

Complementing formalised civic engagement pathways, this dynamic aims to permeate the entire social fabric with formats that are accessible to all. The objective is twofold: to enable every citizen to better understand the information dynamics that structure the public space, while opening up concrete paths to engagement that will nurture the pool of skills needed to defend our democratic institutions.

INTEGRATING THE ISSUES OF COUNTERING INFORMATION MANIPULATION (LMI) INTO EXISTING FRAMEWORKS

Several voluntary engagement mechanisms already in place will be mobilised to disseminate a **culture of civic vigilance and informational resilience** on a large scale.

The **Defence and Citizenship Day (JDC)** will be a key moment to present the fundamental challenges of combating foreign digital interference, in line with the recommendations of the 2024 Senate report on combating malicious foreign influence entitled "*Towards a nationwide mobilisation in the face of the new Cold War*". A summary module will present the technical mechanisms of manipulation and best practices for verification.

The Civic Reserve and Civic Service, as frameworks for voluntary engagement of varying durations, will offer many young people the opportunity to discover professions related to information and the protection of public debate. In conjunction with stakeholders in the sector (media, associations, institutions), **specific assignments** will be offered and promoted.

In this context, the **digital civic reserve** created by Article 23 of the SREN Act of 21 May 2024 will also need to be mobilised in order to fuel and support the collective effort to combat information manipulation. This mobilisation may take the form of disseminating information and insights to the population, but also participating in monitoring, analysis and response activities in the face of threats. Reservists will have privileged access to up-to-date information on current threats, enabling them to strengthen and multiply the capacity for action at the national level.

CREATE PATHWAYS INTO THE CITIZEN AND OPERATIONAL RESERVE FORCES

In order to sustain the skills acquired and capitalise on the volunteers' experience, **structured pathways** will be created to **civic and operational reserves**, enabling commitment to be maintained beyond the initial schemes.

STRATEGIC OBJECTIVE 4. FOSTER A CULTURE OF CIVIC PROTECTION AGAINST INFORMATION MANIPULATION

Foster a civic culture of protection against information manipulation by disseminating participatory awareness-raising formats nationwide, supported by a network of local experts.

Faced with increasingly complex information dynamics and the proliferation of vectors of manipulation, every citizen must have access to the **skills necessary to understand, analyse and respond** to various forms of manipulation and foreign interference. The objective is to **foster the development of critical thinking**, with a view to **empowering and raising awareness in order to fulfil the functions of collective defence**. This ambition requires **multiplying the number of appropriate intervention formats** (workshops, debates, conferences, immersive experiences, etc.), drawing on local, participatory and decentralised dynamics, aimed at all audiences and across the entire territory.

CAPITALISING ON PUBLIC, POPULAR AND CIVIL SOCIETY INITIATIVES

Faced with the growing challenges of information manipulation, **numerous initiatives, ranging from popular education to citizen debate forums, are already working to equip and raise awareness among the entire population.**

Popular education plays a key role in disseminating tools, training and information to understand and protect against information manipulation. Not only does it address digital issues, but it also covers a wide range of fundamental knowledge – scientific, historical and civic – all of which is necessary for the resilience of the population. More recently, the Café IA initiative has begun to offer spaces open to all for discussion, guidance and experimentation on our relationship with AI.

In terms of resources, structures such as CLEMI are an example of well-established forms of mobilisation that contribute to raising awareness of information issues.

Special support should also be given to the contribution and promotion of resources such as Wikipedia, which enjoy a high level of trust and play a central role in how French people verify information, whatever the form of knowledge, as their reliability and quality depend directly on the commitment and size of their communities.

The national strategy will support these diverse dynamics by providing, grouping, gathering or consolidating, as needed, educational resources, designed in conjunction with media and information literacy stakeholders, as well as popular and civic education in general, and by promoting existing local initiatives.

DEPLOY, UNITE AND COORDINATE A NETWORK OF STAKEHOLDERS AND MEDIATORS

Participation in digital mediation, popular education and Café IA-type initiatives depends on the existence of a national network of local stakeholders capable of coordinating spaces that combine discussion and knowledge sharing as close as possible to citizens. Digital mediators play a particularly valuable role, as they help to **maintain links with the most isolated and potentially vulnerable people**. Bringing them together in a **dynamic, supportive and coordinated network** will enable specific outreach work to be carried out.

In the fight against information manipulation, **this network will be enriched by educators and facilitators in media and information literacy** in the context of popular education, actors from the associative and media world involved in civic training, as well as people trained through the LMI Academy, educational and university courses, civic engagement programmes, etc.

The members of this network will be equipped and supported over the long term thanks to a **continuing education** programme, fed by educational resources from scientific or institutional partners co-produced with VIGINUM.

An **information channel** will ensure that knowledge is kept up to date and that weak signals are quickly disseminated. This network will play an essential role in **sharing the keys to understanding, creating automatic responses, and preventing information manipulation** at the local level.

ENGAGING LOCAL AUTHORITIES, THEIR ELECTED REPRESENTATIVES AND LOCAL COMMUNITIES

The effectiveness of the fight against information manipulation will depend on the ability to mobilise the knowledge and capacity for action of elected representatives and local actors. Action taken at the national level should promote autonomy, cooperation and local initiatives. Numerous initiatives, such as the meetings organised as part of NUMÉRIQUE EN COMMUN(S), demonstrate a capacity for mobilisation and collective action at the local level that can be supported at the national level without undermining local dynamics.

Regulate online platforms and generative artificial intelligence services

Develop digital governance by making the key players in the information environment – platforms, search engines, AI service providers – accountable for the systemic risks associated with information manipulation.

PILLAR

02

The contemporary information environment has become an technical ecosystem structured by digital intermediation: search engines, social platforms, chatbots and generative AI tools now organise access to information, the hierarchy and visibility of content, and the formation of public opinion. This algorithmic architecture, which has no equivalent in traditional media governed by clear editorial responsibility, raises unprecedented challenges in terms of integrity, accountability, pluralism and transparency.

The arrival of generative AI technologies, integrated into search engines, social networks, operating systems and digital assistants, further increases the complexity of this environment. These tools enable the production and dissemination of synthetic content on a large scale, but also allow users to bypass information producers, whether verified or not, while feeding off their content.

Faced with the growing dominance of certain platforms and the proliferation of illegal or harmful behaviour, the European Union has adopted ambitious regulations, notably the Digital Services Act (DSA), which requires very large online platforms and search engines to mitigate the systemic risks they pose.

This regulation also provides for better access to data for regulatory authorities, transparency guarantees for users, options for non-personalised feeds, and a strengthened reporting mechanism. In March 2024, guidelines were developed by the European Commission to clarify what was expected of platforms in applying the DSA during election periods.

Subsequently, a toolkit dedicated to elections was developed for national digital service coordinators in order to put in place all the necessary measures for better implementation of the DSA.

In this context, France intends to take the lead in ensuring the rigorous and robust implementation of the European framework and to work actively to improve its operational effectiveness.

In this context, it is imperative to make full use of the legal levers available to take effective action on digital platforms and generative AI services, particularly during election periods (SO5). This involves defining common and precise technical rules at European level enabling national authorities to impose concrete measures on platforms and AI services during election periods – adaptation of recommendation systems, enhanced moderation obligations, transparency requirements – in order to protect public debate. A clear framework makes these interventions legally sound, limits the risk of challenge and ensures their compliance with European law.

Secondly, the strategy aims to establish a rigorous framework of relations and regulation, subject to sanctions, between platforms, generative AI providers, authorities, researchers and civil society (SO6). This structured framework will be at the heart of a collective effort to promote the sharing of analyses, early warnings and remedial practices, with a view to ensuring long-term coordination and pooling of efforts.

France will continue to consolidate its means of analysing AI-related information risks (SO7). Interacting constantly with the work being done to implement the European regulation on AI and with scientific analyses being carried out at national and international level, the interdisciplinary operational platform already set up in France to detect, qualify and anticipate the effects of generative AI on the public space will be strengthened.

Finally, the national strategy will tackle the mechanisms for financing the manipulation of information through programmatic advertising (SO8). To this end, several priorities have emerged: objectifying the phenomenon, supporting the establishment of dedicated benchmarks, and developing audit and traceability tools.

STRATEGIC OBJECTIVE 5. ENSURE THE NECESSARY ROOM FOR MANOEUVRE WITH REGARD TO GENERATIVE AI PLATFORMS AND SERVICES WITHIN THE FRAMEWORK OF EUROPEAN LAW

The importance of generative AI platforms and services in shaping our information environment requires us to mobilise all possible levers offered by the European and national framework.

FURTHERING THE IMPLEMENTATION OF THE EUROPEAN DIGITAL SERVICES REGULATION

The regulation of information society services is still largely based on the principles set out in European Directive 2000/31, known as the “eCommerce” Directive. This Directive affirms, in particular, the **country of origin principle**, according to which only the Member State in which a service is established is competent to impose specific obligations that go beyond harmonised European standards, depending on the degree of harmonisation in the field concerned.

In addition, the European Digital Services Act (DSA) entrusts the European Commission with the primary supervision of very large platforms and search engines, while granting the authorities of the country of establishment exclusive powers over other actors covered by the regulation and providing for coordination mechanisms with and between Member States. In this context, the ability of the Commission and Member States to act to protect national public debate, particularly during election periods, can and must be strengthened.

While Member States have full competence in electoral law, a point of tension has emerged in the assessment of their ability to intervene and impose formal obligations on online platforms. A turning point in case law was initiated by the judgment of the Court of Justice of the European Union in the Google Ireland case (9 November 2023). It recognises that Member States other than the Member State of establishment may take targeted and asymmetrical action, provided that: (i) the measures envisaged are directed at a specifically identified actor; (ii) the measures envisaged are necessary and proportionate to one of the legitimate objectives defined in Article 3(4) of Directive 2000/31; and (iii) the Member State of destination of the service has first established a failure⁴ on the part of the Member State of establishment⁵, after requesting it to take measures and notifying both that State and the European Commission of its intention to take such measures itself. A dialogue with the Commission should clarify the scope for action in this regard in the electoral field.

Within the existing regulatory framework, it is also necessary to continue the work undertaken with the European Commission to specify the specific technical measures that major online platforms should take before, during and after an election.

The guidelines on the protection of minors online and recent developments in age verification for access to social networking services demonstrate that it is possible to find ways of reconciling national legislation with the European framework. Such measures could in future relate to **the regulation of the algorithmic systems of digital platforms during election periods**, and could be deployed when the law of a Member State, in accordance with EU law, prescribes specific communication objectives during election periods on online media. Outside of election periods, they may also focus on the need for algorithmic transparency, the obligation to remove inauthentic accounts, and the regulation of online political advertising, in accordance with the Digital Services Act.

Finally, it is important to anchor the deployment of measures in a rapid, ambitious and demanding

⁴ “Failure” is understood to mean the absence of effective action or the clear inability of the competent authority of the Member State of establishment to exercise its supervisory and enforcement powers, in particular in the event of inaction, unjustified delay or measures that are clearly insufficient in relation to the applicable obligations.

⁵ Refers to the Member State in which the service provider is established for the provision of the service concerned, in principle the location of its registered office or main establishment in the Union, and whose authority has priority under the country of origin principle.

implementation of the DSA, making it possible to:

- achieve a high level of involvement by national authorities in the application of the Regulation at European level;
- explore structural remedies relating to the architecture of platforms and their interaction with third parties that are able to offer alternative recommendation and moderation features, with full application of the obligations applicable to these parties, particularly in terms of systemic risk management, and the implementation of a risk assessment for these new architectures;
- safeguard the initiatives of national authorities aimed at protecting public debate during electoral periods;
- to explicitly address the risks and content arising from generative artificial intelligence services.

ANALYSE AND DRAW CONCLUSIONS ABOUT THE RESPONSIBILITY OF DIGITAL PLATFORMS WITH REGARD TO THEIR ALGORITHMIC SYSTEMS

Through their recommendation and moderation functions, for platforms, and text generation, for generative AI, these services can have a strong influence on the content produced and how it is received by the public. Platforms control the design and parameters of their algorithmic recommendation, personalisation and moderation systems, which must be analysed in light of the criteria established in case law in order to draw all the necessary conclusions, both in terms of the responsibility of these actors with regard to their algorithms and the capacity for action of the competent national authorities in the States where their services are present.

Dominant social networks restrict the emergence of alternative forms of content dissemination, moderation or access beyond those defined by the company itself. Beyond ease of use and the immediate satisfaction offered to users, this structural lock-in may also reflect design or configuration choices that favour, or even amplify, the risks of information manipulation, notably through the exploitation of hidden algorithmic vulnerabilities that must be studied, assessed and brought to light. Mobilising the national and European scientific community for this purpose is now imperative. The competent authorities will seek to document these phenomena within the framework of existing powers, in particular through a dedicated research project aimed at conducting an in-depth analysis of the algorithmic methods implemented by certain very large online platforms.

Finally, structural remedies, such as vertical interoperability⁶ already permitted by Article 6 (7) of the Digital Markets Act (DMA) with regard to operating systems, merit further investigation – within the framework of European instruments and with full application of the obligations applicable to the actors concerned and assessment of the risks specific to these new architectures – **as a means of protecting users from being trapped in a model that is potentially conducive to the manipulation of our information environment.** Alternative solutions for interfaces, recommendations or moderation could then be used to thwart structures or behaviours that favour the manipulation of our information environment.

⁶ Vertical interoperability refers to the ability of third-party services or tools to connect technically to a dominant platform or system in order to offer, on top of its standard functionality, alternative interfaces, recommendation mechanisms or moderation devices. It aims to reduce dependence on the technical and editorial choices of the main player and to allow the emergence of competing or complementary functionalities.

STRATEGIC OBJECTIVE 6. A STRUCTURED DIALOGUE WITH PLATFORMS FOR SHARING INFORMATION WITH PUBLIC AUTHORITIES AND SPECIALISED CIVIL SOCIETY ORGANISATIONS

Establish a permanent framework for dialogue with platforms and AI providers to enable the sharing of information, analyses and feedback with public authorities and civil society specialising in information manipulation.

Beyond the legal developments underway at national and European level, the fight against information manipulation requires a structured framework for exchange between digital platforms, generative AI providers, public authorities and specialised actors (research, verification, OSINT, analysis of information phenomena). Information useful for understanding the mechanisms of manipulation, the uses of platforms and the effects of recommendation systems remains scattered and unevenly accessible. This situation limits the capacity for shared analysis and the structured expression of the needs of specialised stakeholders.

The experience of the Online Hate Observatory run by ARCOM has demonstrated the usefulness of an institutionalised forum for exchange between platforms, authorities and specialist actors, enabling the sharing of analyses, practices and feedback. Based on this model, a permanent framework for structured dialogue with platforms and AI providers will be established, dedicated to information manipulation.

Several sectoral co-regulation frameworks, at both European and national level, based on institutionalised forums for exchange between regulators, private actors and experts, have demonstrated their usefulness in improving the transparency of practices and the circulation of relevant information. For example, the European Union's Code of Practice on Disinformation brings together platforms, research actors and specialised organisations in a structured framework for exchange and transparency, with commitments to reporting and information sharing, and now constitutes a co-regulation mechanism linked to the Digital Services Regulation.

In this context, the establishment of a permanent national framework for structured dialogue with AI platforms and providers aims to fill this gap in organised exchange and provide the ecosystem with a stable space for sharing analysis and knowledge on information manipulation phenomena.

BUILDING A STRUCTURED FRAMEWORK FOR EXCHANGES BETWEEN PLATFORMS, AUTHORITIES AND SPECIALISED STAKEHOLDERS

This framework will take the form of a regular and formalised mechanism for dialogue, coordinated by an identified authority, enabling the circulation of information, the comparison of analyses, and the structured reporting of observations and needs from specialised civil society actors to platforms and public authorities.

Its functions will include, in particular: the sharing of information, analyses, case studies and lessons learned; the pooling of observations and typologies of manipulation; presentations by platforms and AI providers of their practices and developments; the establishment of rapid response mechanisms; and the structured transmission of questions and recommendations from specialised stakeholders.

The Law of 21 May 2024 aimed at securing and regulating the digital space (SREN) has already established, for the needs of the State, a coordination network designed to strengthen information-sharing, cooperation and dialogue between the competent authorities, to address issues relating to the interaction between different regulatory frameworks, and to develop a shared strategic reflection on the challenges of digital regulation.

The proposed mechanism is intended to operate in conjunction with this internal State coordination framework and to serve as its structured extension towards platforms and specialised civil society.

STRATEGIC OBJECTIVE 7. CONSOLIDATE NATIONAL CAPACITY TO ASSESS THE RISKS POSED BY ARTIFICIAL INTELLIGENCE IN THE FIELD OF INFORMATION MANIPULATION

Establish a benchmark expert capability able to assess, quantify and anticipate the systemic effects of artificial intelligence on the reliability of the information environment.

The rise of artificial intelligence (AI), particularly generative technologies and agentic systems, is profoundly redefining the information landscape. While these tools offer new opportunities, they also introduce major systemic risks, particularly in terms of the automated production, amplification and dissemination of content that is manifestly inaccurate or misleading.

Deepfakes, persuasive text generation, voice synthesis, identity cloning and algorithmic micro-targeting: artificial intelligence now makes it possible to manipulate information on an unprecedented scale, in ways that are difficult to detect and at marginal cost. These uses pose direct threats to the sincerity of democratic debate, particularly during elections or in crisis situations.

On the regulatory front, the **European AI Act** introduces a risk classification system based on the potential impact of AI on fundamental rights and security. Certain systems used for the purpose of manipulating information will fall into the category of **high-risk systems**, or even prohibited practices (use of manipulative, deceptive or subliminal techniques). **The obligation of transparency, the labelling of synthetic content, and the traceability of models** constitute a first line of regulatory safeguards.

The **International Scientific Report on the Safety of Advanced AI**⁷ also confirms the growing consensus on the risks that generative models pose to the information environment. In particular, there is scientific consensus that generative models (i) **facilitate mechanisms for manipulating information**; (ii) **facilitate, at the very least, large-scale manipulation of public opinion**, particularly during elections or in crisis situations.

ASSESSING AND RESPONDING TO AI-RELATED RISKS: CREATION OF AN AI x LMI CENTRE OF EXCELLENCE WITHIN VIGINUM

In light of these findings, France must develop a robust, multidisciplinary and coordinated assessment capability based on the research and assessment activities of its National Institute for the Assessment and Security of Artificial Intelligence (INESIA), the government's AI technical expertise services, such as the Digital Regulation Expertise Centre (PEReN), the National Institute for Research in Digital Science and Technology (INRIA) and the National Metrology and Testing Laboratory (LNE), as well as the operational expertise of VIGINUM and the relevant administrations.

To maximise the impact of VIGINUM's contribution to the collective effort, its DATALAB team will be transformed into an AIxLMI centre of excellence. The open-source work carried out by these players will enable, in particular:

- provide turnkey tools and services to **fact-checking communities, the media, NGOs and researchers**;
- **strengthen support for ARCOM** in relation to its responsibilities under the European Digital Services Regulation (moderation and verification of algorithms);
- **produce independent risk assessments**; and support public authorities in developing regulatory or technical responses.

In addition, France must provide support to those involved in the ecosystem who are engaged in analysing and detecting breaches of the integrity of the national information space. This support may

⁷ The International AI Safety Report 2026 is an international assessment of the capabilities and risks of advanced artificial intelligence systems. It was launched following a resolution adopted by 30 countries, as well as representatives from the European Union and the UN, at the AI Safety Summit in Bletchley Park. Inspired by the IPCC model, it brings together a panel of international experts to provide a common scientific basis for public decision-makers.

take the form of calls for cooperation or funding, as well as various means of raising awareness.

STRATEGIC OBJECTIVE 8. CUT OFF THE FUNDING OF FOREIGN DIGITAL INTERFERENCE BY STRENGTHENING TRANSPARENCY IN PLATFORMS' ADVERTISING AND MONETISATION SYSTEMS

Mitigate the systemic risks associated with the economic model of online platforms in terms of foreign digital interference, and reduce the profitability of websites, accounts and channels involved in manipulation or fraudulent practices by increasing the transparency of monetisation systems and the traceability of digital advertising flows.

The business model of large platforms is based on the attention economy, which rests on three pillars: offering free services to attract a massive audience and maximise retention, transforming this audience into behavioural data, and monetising this data through automated advertising technologies. At the same time, monetisation programmes provide remuneration to 'partner' content creators and publishers according to the volume of views and engagement with their publications.

The role of advertising and monetisation mechanisms in the direct or indirect financing of information manipulation has long been documented, notably in academic work, journalistic investigations and the European Code of Practice on Disinformation. However, existing mechanisms have shown their operational limitations and insufficiently binding nature..

Social media recommendation algorithms amplify the content that generates the most activity (clicks, comments, shares, reading time). These metrics, often linked to the emotional charge of the content, give an indirect advantage to polarising or even controversial content. The financial interest represented by the virality of certain topics can thus motivate opportunistic actors. The institutionalisation of redistribution programmes thus creates an 'economy' of manipulation, which can favour actors who massively produce content that is manifestly inaccurate or misleading.

This risk, which has been identified for several years, is intensifying with the rise of generative AI, which lowers the costs of producing and distributing content on a large scale. It does not create the phenomenon, but it does change its scale and speed, which reinforces the challenge of regulating monetisation mechanisms. The fact that certain programmes are limited to audiences in a few countries, including France, increases the risk of opportunistic targeting of French users.

Beyond the platforms' internal monetisation mechanisms, programmatic advertising is a major channel for financing content on the web. Based on automated real-time auctions for the purchase of targeted space, and accounting for nearly 90% of digital advertising expenditure, it has industrialised advertising flows between platforms, intermediaries and third-party publishers (websites, applications, connected environments). However, this automation, optimised for performance and cost, exposes advertisers to the risk of unintentional placement on media with low editorial value or that disseminate information, including when operated by foreign actors.

The European Digital Services Act (DSA) now provides a binding legal framework for addressing systemic risks associated with platforms, including information manipulation, fraudulent use of advertising systems and monetisation mechanisms. Transparency obligations (in particular Articles 26 and 39) and mechanisms for assessing and mitigating systemic risks form the main basis for public action. The strategy is part of this framework and aims to strengthen its operational effectiveness, with a focus on monitoring, auditing and, where necessary, corrective measures and sanctions.

These measures are linked to the DSA's systemic risk management obligations and European investigation and sanctioning procedures, relying on standardised technical mechanisms that guarantee auditability, advertising traceability and public identification of interference media.

MITIGATING SYSTEMIC RISKS OF FOREIGN DIGITAL INTERFERENCE INDUCED BY MONETISATION PROGRAMMES

The strategy first plans to define a national framework mapping the monetisation mechanisms of platforms and to strengthen the application of transparency obligations for creators and publishers based outside France, whether in another Member State or in a third country, who disseminate political content targeting French audiences, in addition to the obligations already provided for in Regulation (EU) 2024/900 on the transparency and targeting of political advertising, particularly when monetisation or promotion mechanisms do not formally fall within the scope of political advertising as defined in that Regulation (location of the actor, signatory to the contract, financial flows, etc.). This framework will serve as a prototype and may be extended to the European level, in accordance with the competences of the European Union and the existing harmonised framework.

Several actions aim to make platforms more accountable:

- require full transparency on commercial relationships with individuals or entities involved in documented foreign digital interference operations, particularly those under EU sanctions;
- require platforms to implement a code of conduct for monetisable content and provide for penalties in the event of non-compliance;
- combat the abuses of influencers and creators linked to foreign digital interference, drawing inspiration from Law No. 2023-451 of 9 June 2023 on the regulation of commercial influence;
- encourage the verification of administrators' identities and the reliability of content for eligibility for monetisation programmes;
- require the suspension of funding for accounts that repeatedly or systematically disseminate misleading information for profit, with transparency regarding the accounts concerned.

A TECHNICAL FRAMEWORK DEDICATED TO THE TRACEABILITY OF ADVERTISING FLOWS

The strategy also provides for the definition of a minimum technical framework to ensure the traceability of digital advertising flows. A compliance grid will be used to assess the presence, completeness and consistency of these elements. This traceability will be essential for auditing campaigns, detecting opaque or fraudulent paths, and limiting the exposure of messages to undesirable contexts.

It will also make it possible to verify compliance with platforms' transparency obligations regarding political advertising, particularly those that are prohibited or contrary to their terms of use prior to national elections.

A PUBLIC REGISTER OF MANIFEST VEHICLES FOR MANIPULATION OPERATIONS

A public register will list websites or channels identified as manifest vehicles for foreign digital interference. It will be based on independent assessments involving journalists, researchers, OSINT experts, independent organisations, and competent state bodies such as VIGINUM. The inclusion criteria will be transparent: the manipulative nature of the content, lack of editorial transparency, and participation in coordinated campaigns.

This register will be freely accessible in interoperable formats (downloadable files and APIs), enabling integration into the tools used by media agencies, advertising platforms and public-sector actors. It will be updated regularly and time-stamped, with an adversarial procedure allowing publishers to challenge their inclusion. This register will not replace the assessment of the legality of content, but will serve as a transparency and accountability tool within a co-regulatory framework.

Strengthen operational capacity to combat foreign digital interference

Develop a sovereign, responsive and credible operational response to information manipulation by consolidating operational capabilities for detection, characterisation, attribution and response, and by strengthening the national technological ecosystem.

PILLAR

03

Ensuring the integrity of public debate in the digital age requires fully operational national capabilities that can detect hostile manoeuvres, understand their motives, and respond to them with responsiveness and discernment. This operational foundation, which is still being consolidated, constitutes the strategic framework for combating foreign digital interference. Faced with the growing threat to information security, France is committed to developing a coherent, graduated and credible response, combining technical, legal, diplomatic and industrial dimensions.

The first condition for effectiveness is shared early detection. This is the objective pursued by strengthening the capabilities for monitoring, detecting and characterising foreign digital interference (SO9). The targeted campaigns, which are increasingly stealthy and hybrid, require continuous and shared vigilance. The COLMI system, transformed into an operational and technical coordination platform, will play a central role in this community. The diplomatic network, particularly through its posts abroad, will provide decisive support for this strategy by ensuring enhanced contextual monitoring in the most vulnerable areas. The strengthening of the monitoring system of the Ministry for Europe and Foreign Affairs (MEAE) will also make it easier to detect influence campaigns and strategic communication by foreign actors.

But detection is not enough: it is also necessary to be able to respond. The second pillar of the strategy is **the development of an interministerial doctrine for responding to foreign digital interference operations and, more broadly, to the manipulation of information originating from foreign sources (SO10).** Placed under the authority of the SGDSN and the MEAE, the interministerial mechanism will, depending on the situation, propose strategies combining different levers – technical, diplomatic, judicial, economic or communication-related. Their concerted mobilisation, including within a multilateral, European or allied framework, will restore public confidence, impose a cost on the aggressor and prevent recurrence.

This response presupposes fluid coordination between the administrations concerned, in compliance with the law and validated policy guidelines, and without prejudice to the specific powers of each administration, which remains capable of acting according to its own prerogatives and legal framework.

This interdepartmental response also relies on a strengthened judicial capacity (SO11). To guarantee its effectiveness, a judicial action plan will be deployed: strengthening the competent public prosecutor's office, increasing the competence of local courts and improving coordination between administrative and judicial services. Particular emphasis will be placed on protecting the electoral process.

Finally, in order to consolidate analysis capabilities over the long term, France is supporting the emergence of a sovereign open-source intelligence sector (SO12). OSINT is an essential lever today, still largely structured by interested, militant, journalistic or academic communities acting outside the institutional framework. The State will promote the development of a trusted technological ecosystem, backed by sovereign tools, secure environments and public-private pathways.

The national strategy will also promote skills developed by the independent OSINT community through concrete mechanisms such as micro-financing, integration into the Academy's activities, and established cooperation networks. This link between citizen expertise and public interest missions will enrich monitoring capabilities and strengthen collective resilience.

STRATEGIC OBJECTIVE 9. STRENGTHEN CAPABILITIES FOR DETECTING AND CHARACTERISING FOREIGN DIGITAL INTERFERENCE

Consolidate the national capacity for continuous, shared and distributed monitoring, detection and characterisation of foreign digital interference, in order to detect hostile campaigns at an early stage and rigorously assess their scope, mechanisms and perpetrators.

Given the growing complexity of information manipulation campaigns, early detection is of paramount importance. Foreign digital interference can take many forms and rely on a variety of vectors: social networks, video platforms, encrypted messaging services, specialised forums, etc.

The operational tempo of countering information manipulation makes it a form of permanent crisis management that requires almost continuous technical exchanges in order to address the threat. For a response strategy to be effective, it is essential to have a reliable and responsive alert and response system based on a collective, high-performance and sovereign monitoring, detection and characterisation capability.

STRENGTHENING THE NATIONAL SYSTEM FOR MONITORING, DETECTING AND CHARACTERISING FOREIGN DIGITAL INTERFERENCE

At the national level, the operational hub for characterising foreign digital interference is COLMI, an operational coordination body led by VIGINUM. To keep pace with adversaries, this structure will evolve into a more permanent set-up, bringing together all relevant technical and strategic stakeholders on a regular basis.

In parallel, a strategic anticipation capability will have to be strengthened in order to prevent the emergence of campaigns. It will rely on a range of cross-cutting methods: open-source intelligence (OSINT), algorithmic processing of large datasets, modelling of propagation dynamics, and expert analysis. Structured partnerships with academia, platforms, and public and private laboratories will further enhance this distributed analytical capability.

The ramp-up of the MEAE's content monitoring capabilities, supported by the diplomatic network, will provide significant capacity in this area.

Finally, interministerial mechanisms (bodies, channels of communication, designation of focal points) will be deployed as necessary to facilitate the flow of information with administrations and institutions that have a role to play in detecting and disseminating information on the methods used to manipulate information.

SUPPORTING DETECTION FROM ABROAD: THE ROLE OF THE DIPLOMATIC NETWORK

International monitoring, detection and characterisation capabilities are a useful complementary lever, particularly in sensitive areas or areas with limited technical coverage. The French diplomatic network, led by the Ministry for Europe and Foreign Affairs in Paris, will be able to contribute to the **reporting of contextual information**, the **identification of hostile actors** and the **issuing of alerts in the event of sensitive periods** (elections, political tensions, targeted information attacks).

To this end, several actions will be encouraged:

- mapping information ecosystems at local and regional level (dominant platforms, narrative relays, hostile actors);
- maintaining regular monitoring of content and strategic channels, beyond institutional actors alone;
- strengthening interministerial coordination to facilitate the sharing of weak signals, align public authorities in their external communication, and share tools.

STRATEGIC OBJECTIVE 10. STRUCTURE AND COORDINATE THE STATE'S RESPONSE TO FOREIGN DIGITAL INTERFERENCE

Define an operational doctrine for responding to foreign digital interference, based on the gradual and coordinated mobilisation of all the levers of the State, and adapted to the specific requirements of election periods.

The fight against information manipulation is not limited to detecting hostile campaigns. It requires the ability to respond resolutely, in accordance with the law, with clearly identified deterrent or corrective effects.

To this end, France relies on a specific interministerial coordination body under the authority of the SGDSN and the MEAE. The aim is not only to manage the consequences of an event, but above all to address its causes by developing **interministerial response strategies** to identified campaigns of foreign digital interference and, more broadly, foreign manipulation of information.

Each interministerial response is tailored to the nature and severity of the interference, its presumed origin, the effectiveness and availability of the levers that can be mobilised, and the relevant national or international cooperation framework.

MOBILISING ALL THE STATE'S RESPONSE LEVERS

This mechanism is based on a comprehensive toolkit for dealing with foreign digital interference, combining several types of levers for action that can be combined, activated gradually or simultaneously, according to different timeframes. These levers may be:

- **communication-related:** fact-checking and corrective actions, mobilisation of opinion leaders and trusted partners, and the regular publication of information bulletins on foreign digital interference;
- **diplomatic:** public condemnations, retaliatory actions, de-escalation channels, confidence-building measures;
- **judicial:** initiation of proceedings against perpetrators or their intermediaries;
- **economic:** activation of national or European sanctions regimes;
- **military:** mobilisation in support of the action of other administrations or implementation of military levers in accordance with the framework and chain of command of operations;
- **technical:** disruption of adversarial technical capabilities, and targeted dissemination of analytical or warning information.

The **choice of whether to attribute an interference operation to a sponsor** – publicly, confidentially, bilaterally or in a coordinated manner – is a strategic tool in its own right. It is decided on the basis of the effects sought: deterrence, diplomatic signalling, public clarification, or the building of an international consensus.

It is within this framework, for example, that new forms of **immediate responses on social media have emerged, such as the FRENCH RESPONSE account established and managed by the MEAE**. Upstream, this dynamic should be supported by the dissemination of communication expertise and practices that empower a wide range of actors to deliver proactive communication through the most appropriate channels and formats. This concerns the diplomatic network, but also, more broadly, other ministries and, beyond them, non-state actors.

Through this **structured response doctrine**, France intends to **impose increasing costs on aggressors**, reduce the incentive to reoffend and demonstrate its ability to protect, in a credible and proportionate manner, **the integrity of its democratic life in the face of hostile campaigns**.

ESTABLISHING A SPECIFIC MECHANISM TO ASSESS AND COORDINATE THE RESPONSE DURING ELECTION PERIODS

During election periods, the State's newly acquired ability to detect and characterise foreign digital interference operations raises a specific public policy issue: intervening to condemn or counter such manoeuvres may influence the democratic debate, while inaction may allow the manipulation of information to flourish, which could clearly alter the integrity of the election.

In this context, this response doctrine is based on a new dedicated mechanism: the Election Coordination and Protection Network (RCPE), coordinated by the General Secretariat for Defence and National Security.

The RCPE brings together the administrations and independent authorities responsible for electoral matters: ARCOM, CNCCFP, the General Secretariat of the Government, the Ministry of the Interior, VIGINUM and the Ethics and Scientific Committee, which is responsible for monitoring its activities. It is responsible for assessing the threat of foreign digital interference during the municipal election period, proposing response measures where necessary, and informing the general public on a regular and periodic basis.

This network, composed exclusively of administrative actors and independent authorities, has no political or partisan function. Its purpose is to objectively analyse the threat and advise the public authorities on the nature, timing and methods of their intervention during the election period, in a context where any action – or lack of action – is likely to have an impact on the democratic debate.

This mechanism thus makes it possible to coordinate, in real time and in a proportionate manner, the administrative, judicial, technical, communication and diplomatic levers that can be mobilised, while respecting the specific competences of each actor. It helps to ensure a consistent, graduated and clear response from the State to attempts at foreign digital interference in the electoral process, while preserving the neutrality of public action and the integrity of the ballot.

Its continuation and extension will be examined in order to ensure the long-term protection of all elections against any form of interference.

STRATEGIC OBJECTIVE 11. STRENGTHEN LEGAL ACTION IN THE FIGHT AGAINST INFORMATION MANIPULATION, PARTICULARLY DURING ELECTION PERIODS

Provide the judicial authorities with the operational means to combat information manipulation in order to effectively identify, prosecute and punish those involved in foreign digital interference campaigns, particularly during election periods.

The fight against foreign digital interference, and more broadly against information manipulation operations, requires a coherent continuum of administrative, diplomatic, technical and judicial actions. In this context, judicial action is an essential lever for deterrence and punishment, making it possible to directly target the human or technical actors involved in hostile campaigns.

To date, there are numerous criminal offences and provisions in the French Civil Code (incitement to hatred, harm to the fundamental interests of the Nation, defamation or insults, manifest alteration of the sincerity of the ballot).

The challenge lies primarily in operationalising the applicable framework so that it can, in practice, provide for repressive measures targeting natural or legal persons who deliberately participate in the automated, mass or coordinated dissemination of manifestly inaccurate or misleading content, in the interests of a foreign power or under its influence, and with the aim of undermining the fundamental interests of the Nation.

Notwithstanding the rapid implementation, within an administrative framework, of removal, blocking or de-indexing measures, this judicial framework must allow for the opening of dedicated investigations that may lead to the issuance of judicial orders to digital platforms, the monitoring of the quality and quantity of the responses provided, the initiation of proceedings against identified perpetrators or intermediaries, and the judicial characterisation of an interference campaign, on the basis of evidence gathered in compliance with the adversarial principle.

Elections are prime targets for foreign digital interference. To preserve the integrity of public debate at one of the most sensitive times in public life, France will set up an operational response mechanism for election periods. This toolbox will include the **aggravating circumstances** provided for in cases of foreign interference.

STRENGTHENING THE JUDICIAL RESPONSE IN ALL ITS DIMENSIONS

In order to make judicial action faster and more effective, particularly during election periods, the strategy will be based on a **legal toolkit structured around targeted changes to applicable law and their effective implementation.**

- **Ahead of elections: strengthening and extending electoral interim relief proceedings** (Art. L. 163-2 of the French Electoral Code) France will continue the operational implementation of the so-called “anti-fake news” interim relief procedure and will undertake the necessary adaptations to **extend its scope to local elections, in particular municipal elections.** The objective is to ensure the availability of a rapid intervention mechanism (within 48 hours) during election campaigns, where content is disseminated online in a deliberate, artificial or automated, and large-scale manner.
- **After the election: strengthening the crackdown on violations of the integrity of the election and taking better account of the foreign nature of the threat** (Art. L. 97 of the French Electoral Code and Art. 411-12 of the French Criminal Code). France will promote the necessary reforms so that the dissemination of false news or fraudulent manoeuvres undermining the integrity of an election can be sanctioned more severely, through a reassessment of the level of penalties provided for in Article L. 97 of the French Electoral Code. It will also pursue the necessary adaptation to extend the application of the aggravating circumstance of foreign interference to this offence, in order to

strengthen the criminal response where the acts serve the interests of a foreign power or fall under its influence.

In addition, to ensure the effectiveness of judicial action, a comprehensive action plan will be deployed around two main pillars:

- **mobilisation of the competent public prosecutors' offices:** the Paris Public Prosecutor's Office has specialised sections with dedicated resources to handle the most complex cases, in close coordination with specialised State services. This mobilisation already relies on a renewed framework of guidance, aimed, on the one hand, at improving the identification of relevant facts and applicable criminal classifications, and, on the other, at strengthening coordination between regional public prosecutors' offices and the Paris Public Prosecutor's Office, which has been granted exclusive jurisdiction enabling the centralised handling of certain offences in order to ensure a coherent, specialised and deterrent criminal response⁸.
- **consolidation of international judicial cooperation:** France will strengthen its commitment to European and bilateral mechanisms to ensure effective coordination of transnational investigations and facilitate extradition procedures.

⁸ Circular of the Minister of Justice dated 26 January 2026 on the mobilisation of the judicial authority in the fight against information manipulation, accompanied by a "focus" document for magistrates concerning the judicial approach to combating information manipulation; circular of the Minister of Justice dated 21 January 2026 on the mobilisation of the judicial authority in the fight against foreign interference.

STRATEGIC OBJECTIVE 12. SUPPORT THE DEVELOPMENT OF THE NATIONAL CAPABILITY ECOSYSTEM FOR OPEN-SOURCE INTELLIGENCE

Develop a French ecosystem of OSINT-dedicated tools, services and skills in support of operations to detect, analyse and counter online information manipulation.

Open-source intelligence (OSINT) has become an essential pillar of public action in the fight against information manipulation. This cross-disciplinary field of expertise relies on the ability to collect, process and analyse large amounts of data from open sources in order to detect weak signals that indicate manipulation. In a context of increasingly sophisticated foreign digital interference, the methodical exploitation of freely accessible data is a strategic capability. It makes it possible to identify malicious campaigns, understand their dynamics and anticipate their spread.

To take advantage of this, **it is essential to have effective, diversified and resilient collection capabilities**, particularly on the web and social networks. The diversity of platforms, the variability of their architectures and the need to operate at near real-time speeds require a high degree of technical agility.

In addition, these environments are constantly evolving: for functional or security reasons, platforms frequently modify their interfaces and restrict automated collection. In this context, **it is no longer sufficient to have a single tool or isolated technology**. A distributed and adaptable set of solutions is required, avoiding any excessive dependence on a single service provider, method or technical format.

France has operational OSINT capabilities, particularly in specialised environments, whether institutional, academic or private. Several national players are developing promising tools and services, illustrating the potential and vitality of the national ecosystem.

However, these initiatives remain too scattered and insufficiently coordinated at the national level. Their potential remains limited by a low level of pooling and the absence of a structuring framework conducive to industrialisation, technological sovereignty and interoperability. Structuring this ecosystem is now a major strategic challenge.

DEVELOP A SOVEREIGN, INNOVATIVE AND RESILIENT OSINT SECTOR

The French industrial landscape already includes several companies offering high-quality, innovative and competitive OSINT solutions. This pool of actors, which is still in a phase of consolidation, deserves full support in order to reach industrial maturity and meet the growing needs of institutions and civil society.

Public intervention in this area is based on at least three major factors:

- **economic:** supporting French companies that create jobs and value in the country in the field of detection and characterisation;
- **technological:** ensuring the resilience and independence of capabilities in a rapidly changing digital environment;
- **security:** ensuring control of technical chains, data protection and compliance with the applicable legal framework.

France affirms its ambition to structure and strengthen a sovereign, innovative and interoperable national OSINT sector capable of meeting the growing needs of public institutions, researchers, journalists and civil society.

This sector will be based on an industrial policy shared according to three principles:

- **pooled technological tools**, designed by French or European players, in compliance with the legal frameworks in force;
- **secure environments** for processing open data, adapted to the uses of analysts;
- **operational pathways** linking public procurement, research laboratories and startups in the sector in order to support innovation.

A structured dialogue between the State and the ecosystem will make it possible to identify priorities, guide strategic investments and promote the pooling of approaches between institutional and civil actors. Existing mechanisms (France 2030, Bpifrance, public procurement) will be mobilised to provide long-term support to companies in the sector.

RECOGNISING AND SUPPORTING OSINT EXPERTISE EMERGING FROM CIVIL SOCIETY

In France, there is a community of OSINT analysts from diverse backgrounds – research, journalism, development and former institutional circles – who contribute independently to the analysis of information phenomena using open sources. These skills represent a valuable contribution to understanding the digital information environment.

Without calling into question their independence or organisational diversity, the national strategy aims to better identify this expertise and to facilitate, where relevant, interactions with public and academic actors.

To this end, various proportionate and non-binding support mechanisms may be considered, such as light-touch arrangements to support targeted work or projects under the France 2030 plan.

Ensure, together
with our allies,
the existence of
a free, open and
secure
information
space

Build a coherent and ambitious international strategy, based on concrete cooperation, support for strengthening democratic capacities and an active presence in standard-setting forums, in order to ensure global resilience to information manipulation.

PILLAR

04

At a time when certain powers are seeking to turn the digital space into a field of ideological and strategic confrontation, France reaffirms its commitment to a free, open, pluralistic and secure information space. With this in mind, France intends to play a leading role in promoting the law, transparency and sovereignty of open and democratic societies. To this end, it will draw on its alliances, partnerships and recognised expertise to structure a diplomacy of informational resilience around four complementary areas of action.

Develop a European response to the information threat: build a federative approach to detection services within the European Union (SO13) in order to have a functional network. France has a recognised operational model, backed by a robust legal framework. As part of the European Democratic Shield promoted by the European Union, France supports the emergence of a European community for countering information manipulation, particularly through the dissemination of operational best practices for detection, support for Member States wishing to strengthen their operational capabilities, the development of interoperability within the European Union in the fight against information manipulation, and the strengthening of cooperation with third countries (candidate countries and neighbouring countries with similar values).

Target capacity-building efforts on the most vulnerable States and areas: define a capacity-building strategy based in particular on a democratic agenda (SO14). In regions where democracy is fragile, manipulation campaigns can have a major destabilising effect. France is therefore committed to helping define a strategy for strengthening operational capabilities, particularly one based on a schedule of critical democratic events (elections, referendums, etc.). This action will draw in particular on existing European Union instruments and bilateral partnerships.

Coordinate the democratic response in multilateral forums: fully mobilise European, transatlantic and UN circles (SO15). Within the European Union, France will continue its active engagement with the European External Action Service, the Commission and the European Parliament to advance a common doctrine on countering information manipulation.

While aware of the difficulties and divisions within international multilateral forums, France will continue to demonstrate its strong commitment to them. Within the G7, it will promote better coordination of national mechanisms, in line with the commitments made under the Code of Conduct for Information Integrity. Within NATO, it will support the integration of information manipulation into the Alliance's doctrine. Within the UN, it will advocate an approach based on transparency, proportionality and information sovereignty, particularly within the framework of the Global Digital Compact and in the work carried out within UNESCO. The same will apply within the OECD, and France will continue to be active in the French-speaking world through the Organisation Internationale de la Francophonie.

Finally, France will need to **invest in forums** that facilitate multilateral dialogue between private and public actors, without becoming dependent on strategic choices that are unfavourable to multilateralism and that may be made by certain States or private actors. At the same time, it will engage with **standard-setting bodies and capability coalitions**, as an increasing part of the regulation of the information space is taking place in technical standardisation bodies.

STRATEGIC OBJECTIVE 13. DEVELOP A COORDINATED APPROACH BETWEEN THE SERVICES RESPONSIBLE FOR DETECTING AND ANALYSING MANIPULATION CAMPAIGNS WITHIN THE EUROPEAN UNION

Build an operational community within the European Union, structured around specialised national agencies, in order to strengthen coordinated detection and collective response to information threats.

In a context of heightened geopolitical tensions and growing digital destabilisation, the European Union has committed to building a European Democracy Shield. This project aims to protect institutional stability, the integrity of electoral processes and trust in public debate. It is based on a central conviction: every Member State must be able to detect and contain, with agility, attempts at foreign digital interference targeting its citizens, institutions or partners.

In this framework, France enjoys particular legitimacy. Its system for combating the manipulation of information in the digital space is a European benchmark. This model enables France to play a driving role in building a shared capability among Member States, based on the principle of subsidiarity, operational cooperation and collective capacity-building.

FOSTERING EUROPEAN EXCELLENCE IN COUNTERING INFORMATION MANIPULATION

The aim is to foster **European excellence in combating information manipulation in the digital environment** by structuring a genuine community between European institutions and Member States, based on three main areas:

- **sharing operational practices and methodologies** within the EU, drawing in particular on the French approach based on the analysis of inauthentic behaviour and open-source research.
- **supporting Member States wishing to strengthen their capabilities** and promoting the establishment of operational government agencies or services dedicated to detecting and countering information manipulation.
- **strengthening networking and interoperability** between Member States, European institutions and civil society in order to improve cooperation and promote knowledge sharing on information threats.

These priorities aim to strengthen a community of actors involved in combating information manipulation (Member States, EU institutions and civil society), capable of detecting, assessing and documenting information threats with territorial granularity and a shared understanding. This will constitute one of the foundations of the European Democratic Shield, intended to establish a collective capacity to respond to information manipulation originating from foreign actors, while respecting the sovereign prerogatives of Member States in protecting their national debates.

STRATEGIC OBJECTIVE 14. DEFINE A STRATEGY TO STRENGTHEN OUR PARTNERS' CAPACITY FOR ACTION

Build targeted and coordinated international support for countering information manipulation, based on sensitive democratic deadlines, critical geopolitical contexts and local demand for capacity building, in close conjunction with existing European mechanisms.

As foreign digital interference campaigns become more sophisticated, they are increasingly targeting democratic processes directly: national elections, referendums, citizen consultations, and major legislative or social debates. These sensitive periods are becoming prime targets for hostile foreign powers, which see them as opportunities for polarisation, destabilisation, increased confusion or chaos, and ultimately a loss of confidence in institutions.

To respond to this threat, France is already providing support and will further develop support for foreign partners capable of taking action against information manipulation in order to strengthen national capacities ahead of and during critical democratic periods, where requested by the States concerned.

SOLIDARITY-BASED, AGILE SUPPORT ROOTED IN EUROPEAN PARTNERSHIPS

This strategy will be based on several levers:

- **the development of a shared agenda of high-risk democratic deadlines**, led by the MEAE, the European External Action Service (EEAS), the European Union and other international partners, to map areas of vulnerability and anticipate the needs of our allies.
- **the creation of technical support missions**, mobilising French and European expertise, which can be deployed rapidly at the invitation of a State, before or during an election.
- **the consolidation of a European pillar for capacity building** in the fight against information manipulation, particularly as an extension of the European Democratic Shield. This pillar will ensure coordination of efforts between Member States and European institutions.

MAKING EUROPE AN EXPORTER OF INFORMATIONAL STABILITY

By integrating this action into the European framework, France intends to make the Union a hub for the projection of democratic stability. This means anchoring **capacity-building to counter information manipulation in the European Union's external policy instruments**, similar to what already exists for cybersecurity and the protection of electoral processes. The French strategy will promote:

- **the systematic integration of countering information manipulation into European Union-funded electoral assistance or rule-of-law capacity-building programmes;**
- **the creation of countering information manipulation modules within European technical assistance programmes** where this is still needed;
- **the continued development of a pool of European experts in countering information manipulation** who can be rapidly mobilised internationally, within a framework of joint responses to threats.

This effort will build on the partnerships already developed by France in areas of informational or democratic tension, particularly in the Balkans, Eastern Europe and, more broadly, the European Union's neighbourhood.

STRATEGIC OBJECTIVE 15. PRIORITISE FRENCH ENGAGEMENT IN MULTILATERAL FORUMS

Make France a leading and structuring voice in multilateral forums to embed countering information manipulation within a shared vision based on the rule of law, transparency and democratic resilience.

The fight against information manipulation cannot be left solely to national policies. By definition, foreign digital interference campaigns involve international dynamics, target fragmented public opinion and rely on transnational vectors. In this context, multilateral forums are an essential strategic lever for developing common standards, promoting coordinated responses and advancing a democratic vision of the global information space.

STRENGTHENING FRANCE'S PRESENCE AND INFLUENCE IN MULTILATERAL FORUMS

Within the European Union, France is fully committed to the European Democracy Shield agenda, which is based on a dual approach of internal resilience and external influence. It will continue to support the strengthening of the role of the European Commission and the European External Action Service in monitoring, assessing and responding to hostile campaigns. In particular, it will propose consolidating the channels for reporting information between Member States and improving coordination between national capabilities (such as VIGINUM) and European rapid response mechanisms, particularly during election periods.

At the OECD, France will continue the extensive work carried out with a view to strengthening democracy and the integrity of information. The recommendations adopted on this subject on 17 December 2024 provide a framework for action that should be followed.

Within the G7, France will continue to support and contribute to political coordination mechanisms to counter hostile information campaigns, drawing on best practices shared among members and formats for exchange and cooperation such as the *G7 Rapid Response Mechanism*. This forum offers a valuable opportunity to align doctrines, share weak signals, harmonise practices and defend common principles with a view to codification and sharing.

At the United Nations, France will speak with a clear voice in the relevant forums, notably UNESCO and the Global Digital Compact, to have the various forms of information manipulation recognised as a multilateral priority area of action for security, peace and democracy. It will oppose any attempt by authoritarian states to capture the multilateral discourse in order to legitimise censorship or total control of the digital space. In return, it will promote recognition of democratic norms for intervention: proportionality, accountability and the right to information and transparency.

Within NATO, France will strengthen its contribution to work on responding to hybrid threats. In particular, it will support the efforts of the StratCom Centre of Excellence based in Riga, while promoting a more proactive approach to public attribution and coordinated response to manipulation campaigns against Allies.

Affirming its support for a strong and effective multilateral framework, France will continue to be fully involved in the relevant forums. France will also need to **engage in broader forums** that facilitate open dialogue between private and public actors, without being dependent on strategic choices that may be made by certain states and that are detrimental to multilateralism.

Furthermore, within the French-speaking world, the **Organisation Internationale de la Francophonie** is working extensively on these issues and thus provides a framework for sharing relevant information and action, which must continue to be invested in, in conjunction with other multilateral forums.

Finally, information manipulation is not only a political or security issue: it is also a normative and technical challenge. Most of the rules governing the digital space – content formats, chains of trust, authentication protocols, monetisation rules, algorithmic structures – are defined in technical forums that shape global information balances. In these arenas, France must defend a vision based on

transparency, engineering ethics, digital sovereignty and democratic resilience.

Through this multilateral strategy, France intends to articulate its national interests and fundamental democratic principles by contributing to the emergence of an international framework based on the integrity of public debate, algorithmic transparency, the information sovereignty of peoples, transparency and shared security.



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

Secrétariat général
de la défense
et de la sécurité nationale

51, boulevard de La Tour-Maubourg - 75007 Paris
N 48°51'23,5" E 2°18'43,2"
www.sgdsn.gouv.fr