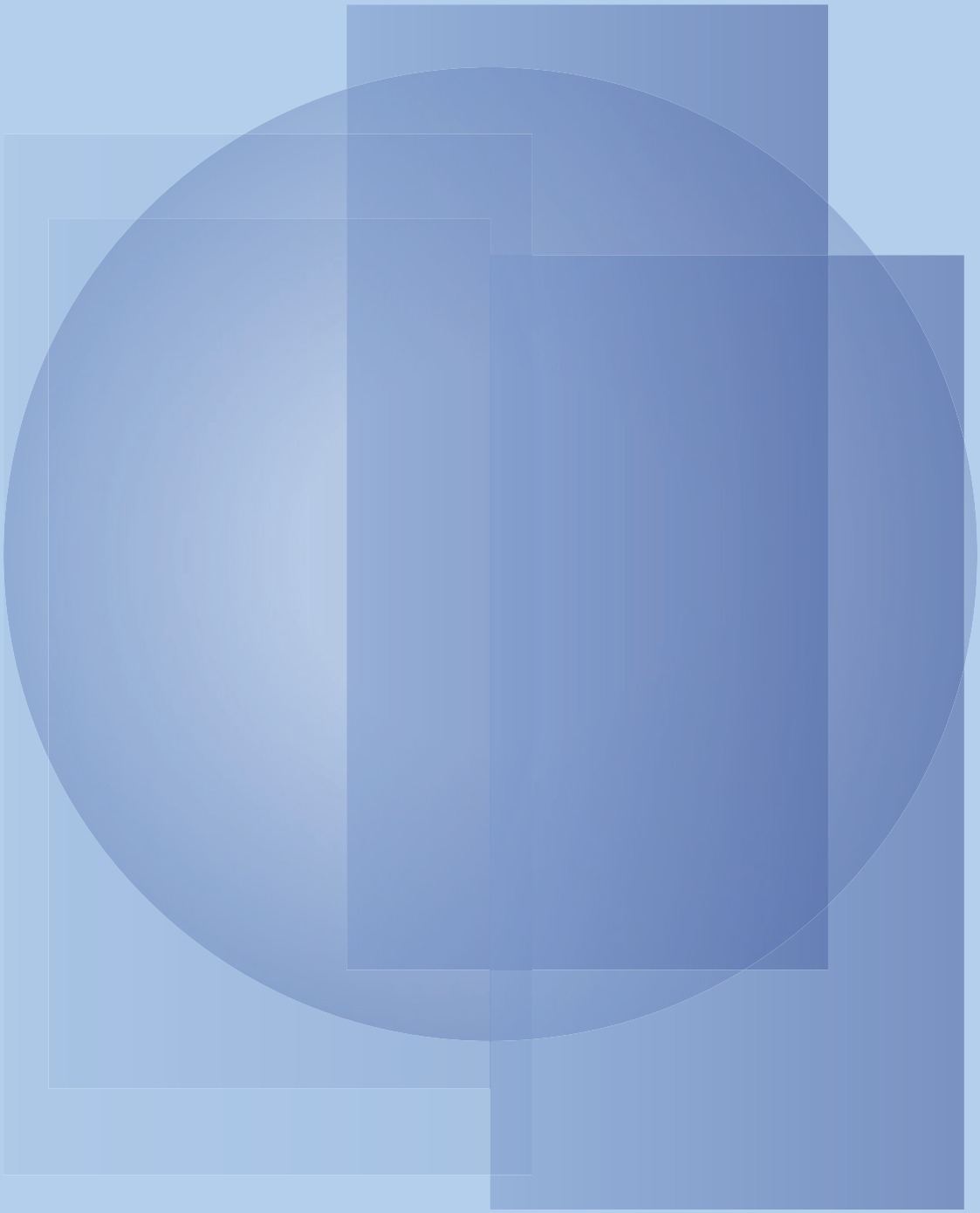
RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

STRATÉGIE NATIONALE DE LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION D'ORIGINE ÉTRANGÈRE 2026 — 2030



PRÉFACE

Notre époque a fait de l'information un bien commun aussi essentiel que fragile. Jamais l'humanité n'a disposé d'un tel accès aux savoirs, jamais la parole n'a circulé avec une telle liberté, jamais l'expression individuelle n'a été aussi immédiate. Cette ouverture est l'une des plus grandes conquêtes de notre temps. Elle est aussi l'une de ses vulnérabilités, car ce que nos sociétés offrent de plus précieux – la liberté d'opinion, le pluralisme, la transparence, le bon sens et la foi en la vérité – peut être détourné par ceux qui cherchent à exploiter leurs failles plutôt qu'à respecter leurs principes.

Les manipulations de l'information ne sont plus des accidents marginaux du débat public. Elles sont devenues des instruments à part entière de confrontation stratégique. Elles visent moins à convaincre qu'à désorienter, moins à imposer une vérité qu'à dissoudre les repères communs, moins à gagner un débat qu'à affaiblir la possibilité même du débat. En brouillant les frontières entre le vrai et le faux et en exploitant les fractures sociales et émotionnelles, elles cherchent à miner de l'intérieur ce que les démocraties ont de plus robuste : la confiance.

Face à ces pratiques, la tentation pourrait être grande d'ériger des murs, de restreindre la parole, de surveiller les idées. Ce serait une erreur. La force des régimes autoritaires est de pouvoir contrôler l'information ; la force des démocraties est de pouvoir la confronter. Là se situe notre ligne de crête : protéger sans censurer, défendre sans contraindre, agir sans trahir ce que nous sommes. La réponse ne peut être ni l'impuissance, ni la fermeture. Elle doit être la lucidité et la responsabilité.

La France fait le choix d'une voie exigeante : celle qui refuse la naïveté sans renoncer à la liberté, celle qui combat les manœuvres hostiles en identifiant leurs auteurs et leurs vecteurs, sans jamais soupçonner les citoyens, celle qui traite les ingérences comme une menace stratégique tout en plaçant la souveraineté populaire au cœur de sa réponse. Il ne s'agit pas de dire ce qu'il faut penser, mais de garantir que chacun puisse penser librement.

Cette stratégie repose sur une conviction simple : le premier rempart contre la manipulation est la société elle-même. Une société instruite, capable de discernement, confiante dans ses institutions et dans ses médias, est une société moins vulnérable aux récits de division. Elle appelle un effort collectif pour renforcer ensemble la capacité globale d'analyse, de signalement et de réponse.

Nous savons que les démocraties sont aujourd'hui observées, testées, parfois attaquées par des régimes qui redoutent leur exemple. Ce n'est pas un hasard si les manipulations de l'information prospèrent d'abord là où existent l'ouverture, le débat et la pluralité. C'est le paradoxe de la liberté : elle attire ceux qui veulent l'affaiblir. Mais c'est aussi sa force : elle permet de leur résister sans leur ressembler.

En adoptant cette stratégie nationale de lutte contre les manipulations de l'information, la France affirme une ambition claire : mobiliser la Nation pour renforcer la résilience de notre démocratie ; engager les plateformes numériques et les services d'intelligence artificielle afin de protéger le débat public ; consolider nos capacités nationales de détection, d'attribution et de réponse face aux ingérences numériques étrangères ; et agir avec nos partenaires européens et internationaux pour garantir l'existence d'un espace informationnel libre, ouvert et sécurisé, où l'on débat sans peur et où l'on décide sans être trompé.

Sous l'autorité du Premier ministre, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) en assurera la coordination et s'appuiera notamment sur le service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM) pour en analyser les manifestations, les détecter, les caractériser et contribuer à la réponse, au service de la protection de notre débat public.

Il ne s'agit pas seulement de protéger nos institutions. Il s'agit de défendre la capacité de chacun à se forger un jugement éclairé. Il s'agit aussi d'affirmer que les manipulations organisées du débat public engagent la responsabilité de ceux qui les conçoivent et de ceux qui les relaient sciemment. Car une démocratie ne se mesure pas seulement à ses lois ou à ses élections, mais à la qualité du lien qui unit la société à l'information, à la confiance et à la liberté.

C'est ce lien que nous devons, collectivement, préserver et renforcer.

Emmanuel MACRON

SOMMAIRE

SYNTHÈSE EXÉCUTIVE

À l'heure où les manipulations de l'information se multiplient, se complexifient et s'intensifient à l'échelle mondiale, la France affirme une stratégie ambitieuse pour protéger son débat public, renforcer la résilience de sa démocratie et agir au sein d'un environnement informationnel libre, ouvert et sécurisé. Tout en s'inscrivant dans une nécessaire approche holistique des mécanismes de manipulation de l'information, cette stratégie repose sur quatre piliers structurants, déclinés en quinze objectifs stratégiques (OS), qui définissent les leviers d'une politique nationale et internationale cohérente, opérationnelle, républicaine et démocratique de lutte contre les ingérences numériques étrangères.

Pilier 1. Mobiliser la Nation pour renforcer la résilience

Le premier rempart face aux manipulations de l'information est la société elle-même. Pour armer la société contre les menaces informationnelles, la France déploie une stratégie de formation, d'engagement et de sensibilisation à grande échelle. Elle vise d'abord à structurer une **capacité nationale d'expertise, notamment** à travers la création de l'**Académie de la lutte contre la manipulation de l'information** au sein du service de vigilance et de protection contre les ingérences numériques étrangères, VIGINUM (**OS1**), puis à bâtir une **filière éducative et de recherche dédiée** à la résilience informationnelle (**OS2**). L'État mobilisera également les **dispositifs d'engagement civique** (Journée Défense et citoyenneté, service civique, service militaire volontaire, réserves) pour former et ouvrir sur un cadre d'engagement dédié (**OS3**). Enfin, une **culture citoyenne assurant une résilience collective face aux ingérences numériques étrangères** sera construite par le recours à des formats décentralisés et participatifs, portés par un réseau d'acteurs locaux (**OS4**).

Pilier 2. Réguler les plateformes en ligne et les services d'intelligence artificielle générative

Le débat démocratique ne peut être préservé sans une action forte sur les architectures numériques qui façonnent la circulation de l'information. La France continuera de jouer un rôle moteur, notamment en période électorale, dans le cadre de la mise en œuvre du DSA, le règlement européen sur les services numériques (**OS5**), en particulier s'agissant de ses obligations de retrait de contenus illicites, de retrait de comptes inauthentiques et de transparence algorithmique. Un **cadre national de coopération** sera mis en place pour organiser le partage d'information et la coordination de l'action avec et sur les services numériques (**OS6**) qui doivent pleinement assumer leurs responsabilités propres. Elle renforcera aussi sa capacité d'analyse des **risques systémiques liés à l'IA** (**OS7**), tout en s'attaquant à un angle mort majeur : **les systèmes de publicité et de monétisation des plateformes**, avec des mécanismes concrets de traçabilité et d'identification des plateformes manifestement impliquées dans des opérations d'ingérence numérique étrangère (**OS8**).

Pilier 3. Renforcer la capacité nationale opérationnelle de lutte contre les ingérences numériques étrangères

Assurer l'intégrité du débat public numérique exige une capacité d'action opérationnelle souveraine, réactive et crédible. La France structurera une **capacité distribuée de veille, de détection et de caractérisation**, fondée sur un réseau d'acteurs institutionnels publics et territoriaux, le renforcement de l'instance de coordination opérationnelle animée par VIGINUM (le COLMI) et l'intégration du réseau diplomatique et militaire (**OS9**). Une **doctrine interministérielle de réponse** aux ingérences numériques étrangères, coordonnée, permettra de mobiliser tous les leviers – techniques, diplomatiques, judiciaires – de manière

proportionnée et coordonnée, notamment en période électorale (**OS10**). **En articulation avec la réponse administrative**, cette approche s'appuiera également sur un **renforcement de la réponse judiciaire**, dont un plan d'action pour les parquets et une meilleure coopération internationale (**OS11**). Enfin, la France accompagnera l'émergence d'une **filière de renseignement en source ouverte (OSINT)**, en structurant un écosystème d'outils, de compétences et de coopération public-privé, tout en soutenant la communauté indépendante des analystes (**OS12**).

Pilier 4. Assurer, avec nos alliés, l'existence d'un espace informationnel libre, ouvert et sécurisé

La lutte contre les manipulations de l'information est un enjeu global. La France s'engage à structurer une **communauté européenne de la lutte contre la manipulation de l'information**, fondée sur la subsidiarité et l'interopérabilité, en faisant notamment émerger un réseau européen de services en charge de lutter contre les ingérences numériques étrangères (**OS13**). Elle développera une **stratégie d'assistance capacitaire**, alignée sur les échéances démocratiques critiques, en appui aux États les plus exposés (**OS14**). Dans les enceintes multilatérales – **UE, G7, OTAN, OCDE, ONU, Francophonie, enceintes de standardisation et hybrides** – la France portera une doctrine démocratique de réponse aux manipulations et travaillera à la consolidation d'alliances (**OS15**).

En somme, cette stratégie entend faire de la France une démocratie résiliente face aux menaces informationnelles contemporaines. Elle s'appuie sur une mobilisation de la population, un engagement interministériel coordonné, une coopération étroite avec les acteurs territoriaux, éducatifs, industriels et scientifiques, ainsi qu'un engagement actif dans les enceintes européennes et internationales. À travers cette politique, la France entend se doter des moyens nécessaires pour, d'un même tenant, défendre et enrichir sa démocratie.

DIAGNOSTIC

En démocratie, l'accès à une information fiable, indépendante et pluraliste est essentiel. Aujourd'hui, à l'ère des plateformes numériques, les possibilités de production, de diffusion et d'expression de l'information ont atteint un niveau inégalé dans l'histoire de l'humanité. Si ces nouvelles fonctionnalités, offertes par la technologie, ont été présentées comme un renouveau de notre débat public, elles ont paradoxalement apporté un risque de manipulation induit par le fonctionnement d'algorithmes conçus par quelques acteurs extra-européens dominants, ainsi qu'une menace d'ingérence numérique étrangère liée à l'exploitation malveillante de ces mêmes fonctionnalités. Ainsi, l'intégrité de notre débat public en ligne se trouve structurellement affaibli, mettant en péril l'expression de certaines de nos libertés.

Face à ce constat préoccupant, une stratégie nationale de lutte contre la manipulation de l'information ne peut ni ne doit prétendre encadrer l'ensemble des dynamiques de circulation des contenus. Elle n'a pas pour objet de surveiller, contrôler ou normer la pluralité des expressions constitutive du débat démocratique. Toute action publique dans ce domaine s'inscrit dans le respect des principes constitutionnels, des droits fondamentaux, des exigences de proportionnalité et des libertés d'expression, de communication et d'opinion.

Aussi, la présente stratégie se concentre prioritairement sur les actions intentionnelles et coordonnées de manipulation de l'information de la part d'acteurs étrangers, en particulier les ingérences numériques étrangères, volet numérique de la manipulation de l'information, intégré au sein de stratégies hybrides malveillantes. Dans cette perspective, l'action publique porte sur les comportements inauthentiques et les chaînes de diffusion (opacité, coordination, amplification artificielle, monétisation) plutôt que sur les contenus eux-mêmes. Elle vise à préserver les conditions d'un débat public libre et ouvert, au sein d'un environnement informationnel sécurisé, pluraliste et transparent.

Face à ces menaces, il revient à l'État d'agir. Non pour encadrer le contenu des opinions ou juger de la légitimité des expressions, mais au contraire pour garantir les conditions mêmes d'une agora souveraine, où l'information, les idées et les opinions circulent librement. L'objectif est clair : défendre la capacité des citoyens à se forger une opinion libre, à participer au débat démocratique, et à faire des choix éclairés au sein d'un environnement informationnel sûr, pluraliste et transparent.

Dans cet esprit, la présente stratégie ne repose pas sur une conception normative ou prescriptive du discours. Elle a pour objectif de consolider les fondements de notre démocratie en agissant sur les phénomènes de manipulation intentionnelle de l'information, et non sur le contenu des opinions : la liberté d'informer et d'être informé, la transparence de l'espace public, et la confiance entre citoyens et institutions. Toute action envisagée dans ce cadre s'inscrira dans le respect scrupuleux du cadre normatif national, européen et international applicable.

LA FRANCE, PAYS PRÉCURSEUR DANS LA RÉPONSE AUX MANIPULATIONS DE L'INFORMATION

Convaincue de la nécessité d'agir, la France a fait de la lutte contre les manipulations de l'information une priorité nationale. Dès 2018, les pouvoirs publics ont pris de premières mesures de lutte contre les manipulations de l'information à travers la mise en place d'un réseau de coordination interministérielle, placé sous l'égide du SGDSN, destiné à mieux appréhender cette nouvelle menace. Parallèlement, l'arsenal législatif a été renforcé par le vote de la loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, qui a doté l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) et le juge des référés de nouvelles prérogatives en la matière.

Depuis lors, la France a développé des atouts structurants : une doctrine, une capacité interministérielle, un cadre juridique stabilisé et une expertise opérationnelle reconnue. La création de VIGINUM en 2021 au sein du SGDSN a permis de structurer cette capacité et de renforcer la crédibilité de la France dans les coopérations internationales.

Cette vision s'est consolidée à mesure que l'État s'est confronté à un terrain numérique marqué par ces menaces. Cette résolution a permis à la France de se doter d'une culture forte et de capacités opérationnelles lui permettant d'assurer la préservation de ses intérêts.

La prise de conscience s'est désormais étendue à l'ensemble de l'écosystème : gouvernements, organisations internationales, acteurs privés et société civile ont multiplié les initiatives. La France prend une part active à ces dynamiques, notamment dans les enceintes européennes et multilatérales.

Dans le champ informationnel, la France a fait le choix de se déployer dans trois domaines distincts : l'influence, la lutte informationnelle et la lutte contre la manipulation de l'information, seul domaine directement visé par la présente stratégie.

L'INFLUENCE

L'influence résulte d'une stratégie proactive explicite, ouverte et assumée visant à agir sur les perceptions étrangères pour façonner un environnement favorable aux intérêts nationaux. Érigée en fonction stratégique par la REVUE NATIONALE STRATÉGIQUE, elle est aujourd'hui essentielle à l'expression de notre puissance et à notre capacité à contrer nos compétiteurs sur tout le spectre de l'hybridité.

Cette logique inclut tant la communication diplomatique traditionnelle que des enjeux nouveaux de riposte, de rayonnement et de gestion des menaces informationnelles, qu'elles soient d'origine authentique ou inauthentique.

Sous la direction du ministère de l'Europe et des Affaires étrangères, une gouvernance spécifique a été mise en place. Ce dispositif a pour objectif de concevoir et de mettre en œuvre des manœuvres d'influence en direction de nos compétiteurs stratégiques.

LA LUTTE INFORMATIONNELLE ET LA LUTTE INFORMATIQUE D'INFLUENCE

La lutte informationnelle participe directement aux manœuvres d'influence. Elle répond à une logique de rapport de force et vise à prendre l'ascendant face à des adversaires désignés pour produire des effets préalablement identifiés.

Dans le champ numérique, la lutte informatique d'influence (LII) constitue un volet des opérations militaires menées dans l'environnement informationnel. Placée sous la responsabilité du chef d'état-major des armées, pilotée par le ministère des Armées et conduite par le COMCYBER, elle agit sur les perceptions et les comportements pour détecter et contrer les atteintes visant, spécifiquement nos armées ou nos intérêts militaires.

La LII s'inscrit à la fois dans la posture permanente d'influence et dans celle de cyberdéfense. Menée exclusivement hors du territoire national, elle peut être conduite de manière autonome ou coordonnée. Elle contribue ainsi à la communication stratégique, à l'analyse de l'environnement des opérations militaires en cohérence avec la stratégie des armées.

LA LUTTE CONTRE LA MANIPULATION DE L'INFORMATION

UNE LUTTE PORTÉE AU NIVEAU INTERMINISTÉRIEL

À la fin de l'année 2020, l'assassinat de Samuel Paty a marqué un tournant dans la perception de la menace, révélant la dangerosité des dynamiques de haine amplifiées numériquement. Ce choc a entraîné, à la demande du Président de la République, la création de la *task force* interministérielle « Honfleur », dont les travaux ont jeté les bases d'un dispositif de réponse pérenne.

Cette volonté politique s'est concrétisée par le décret du 13 juillet 2021 créant, au sein du Secrétariat général de la défense et de la sécurité nationale (SGDSN), le service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM). Ce passage d'une logique de gestion de crise à une structure permanente inscrit désormais la protection du débat public francophone au cœur de la défense et de la sécurité nationale.

Brique centrale de la stratégie nationale, **VIGINUM** détecte et caractérise les opérations d'ingérence numérique étrangère susceptibles de porter atteinte aux intérêts fondamentaux de la Nation. Sous l'autorité du Premier ministre, le SGDSN assure la coordination stratégique de cette lutte. En liaison avec les ministères concernés, il est chargé d'identifier les opérations d'ingérence et d'animer les actions de protection et de réponse interministérielles.

UNE LUTTE ARTICULÉE AUTOUR DE LA NOTION D'INGÉRENCE NUMÉRIQUE ÉTRANGÈRE

Le décret du 13 juillet 2021 a formalisé la notion d'ingérence numérique étrangère (INE) en tant qu'« *opération impliquant, de manière directe ou indirecte, un acteur étranger (étatique ou non), et visant la diffusion artificielle ou automatisée, massive et délibérée d'allégations ou imputations de faits manifestement inexactes ou trompeuses, de nature à porter atteinte aux intérêts fondamentaux de la Nation.* ».

Ce texte fonde une typologie rigoureuse de la menace, qui repose sur quatre critères cumulatifs : une atteinte potentielle aux intérêts fondamentaux de la Nation ; une allégation ou imputation de fait manifestement inexacte ou trompeuse ; une diffusion, ou une volonté de diffusion, artificielle ou automatisée, massive et délibérée ; l'implication, directe ou indirecte d'un acteur étranger (étatique, paraétatique ou non-étatique).

LE CADRE TERMINOLOGIQUE EUROPÉEN ET INTERNATIONAL

La notion française d'INE s'inscrit dans un cadre international structuré autour du concept de **FIMI** (*Foreign Information Manipulation and Interference*).

- **L'Union européenne (SEAE),** définit les FIMI comme des activités intentionnelles et coordonnées, menées par des acteurs étatiques ou non, ayant un impact négatif sur les valeurs et processus politiques. Cette définition fait référence au sein du G7 (RRM).
- **L'OTAN,** utilise une « boîte à outils FIMI » pour décrire les activités manipulatrices visant l'Alliance et ses Alliés, incluant la désinformation et les opérations informationnelles.
- **L'OCDE,** cible les efforts coordonnés pour le compte d'une puissance étrangère visant à corrompre la prise de décision et la parole publique.

UN ARSENAL JURIDIQUE COMPLET : DU SOCLE RÉPUBLICAIN À LA RÉGULATION NUMÉRIQUE

La lutte contre les manipulations de l'information s'inscrit dans la continuité d'un cadre juridique qui a progressivement évolué sous l'influence des nouvelles technologies mais dont l'objectif inchangé demeure de concilier liberté d'expression, protection des droits des personnes comme de l'ordre public et poursuite de l'intérêt général.

- **Le socle de la loi de 1881 sur la liberté de la presse,** qui traduit l'équilibre entre liberté d'expression et responsabilité dont l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 constitue le fondement. Tout en réaffirmant le principe de la liberté d'expression – en prévoyant en son article 1er que « L'imprimerie et la librairie sont libres » – elle en réprime les abus, y compris lorsque ceux-ci résultent d'une expression publique (par opposition à une publication par voie de presse) et prennent source dans la diffusion de « nouvelles fausses » : son article 27 sanctionne ainsi spécifiquement la publication ou la reproduction de nouvelles fausses lorsqu'elles sont faites de mauvaise foi et qu'elles troublent ou sont de nature à troubler la paix publique.

  La loi réprime également d'autres abus de la liberté d'expression n'ayant pas de rapport immédiat avec la véracité du propos tenu, notamment la diffamation et l'injure (définis à l'article 29 et réprimés respectivement aux articles 32 et 33).

- **La loi de 1986 relative à la liberté de communication** a adapté les obligations applicables aux entreprises de presse aux spécificités de la communication audiovisuelle. Tout en rappelant que la communication est libre (article 1er), elle prévoit diverses obligations applicables aux médias audiovisuels, notamment destinés à préserver un débat politique équitable et crée un régulateur à même de sanctionner les manquements : l'ARCOM.

Ce cadre, conçu avant l'ère numérique, demeure le socle normatif de référence dont les grands équilibres sont demeurés inchangés. Il a été complété par des outils adaptés à l'environnement technologique actuel :

- **la loi du 22 décembre 2018 a posé la première définition légale de la manipulation de l'information en contexte électoral,** ciblant les allégations ou imputations de fait manifestement inexactes ou trompeuses diffusées de manière délibérée, artificielle ou automatisée et massive afin d'altérer la sincérité d'un scrutin (Art. L. 163-2 du code électoral). Cette initiative complète un régime de protection des scrutins préexistant : visant à assurer la sincérité du débat démocratique l'article L. 97 du code électoral réprime les manœuvres frauduleuses, telles que la diffusion de fausses nouvelles ou de calomnies, ayant pour but de détourner les suffrages ou de déterminer l'abstention des électeurs ;
- **le Règlement européen sur les services numériques (DSA),** pleinement applicable depuis 2024, qui responsabilise les plateformes en leur imposant d'atténuer les « risques systémiques » pesant sur le discours civique et la sécurité publique (Art. 34). Il est complété par le **Code de conduite sur la désinformation**, qui lie les signataires (plateformes, acteurs de la publicité, société civile) à des engagements précis en matière de transparence du financement publicitaire, de lutte contre les comptes inauthentiques et d'accès des chercheurs aux données des plateformes.

Au-delà des textes dédiés au numérique et aux scrutins, le droit français comporte également un socle de lois transverses qui agissent comme des barrières contre ces manœuvres étrangères :

- **au niveau national (Cohésion sociale)** : les lois contre le racisme, l'antisémitisme et la haine en ligne (1972, 1990, 2021) sont essentielles. Les stratégies d'ingérence exploitent systématiquement nos fractures identitaires pour polariser l'opinion. En réprimant ces discours, le droit français réduit la capacité des acteurs étrangers à transformer nos débats internes en leviers de déstabilisation.
- **au niveau européen (Liberté des médias)** : *l'European Media Freedom Act* (EMFA) de 2024 suit la même logique de résilience. En protégeant l'indépendance des rédactions et en empêchant les

plateformes de supprimer arbitrairement des contenus journalistiques, il garantit l'accès des citoyens à une information fiable, ce qui constitue un élément de résilience face aux manipulations de l'information.

ÉVOLUTION DU PAYSAGE INFORMATIONNEL : LA NUMÉRISATION CROISSANTE DE NOTRE DÉBAT PUBLIC

DU MODÈLE ÉDITORIAL AUX PLATEFORMES NUMÉRIQUES

L'émergence des médias traditionnels, qu'il s'agisse des médias audiovisuels ou de la presse, a été accompagnée par un ensemble normatif stabilisé au niveau national composé de notre bloc de constitutionnalité, du code électoral, de la loi de 1881 sur la liberté de la presse, ainsi que de la loi de 1986 sur la communication audiovisuelle. Autant de règles destinées à garantir un équilibre entre la liberté d'expression, la régulation des supports d'expression publique, et la préservation de l'intérêt général. Ce cadre a été conçu pour des acteurs identifiables, des chaînes éditoriales structurées et des responsabilités clairement établies.

Depuis lors, notre environnement informationnel a été bouleversé par la numérisation et l'algorithmisation des canaux de communication. La capacité désormais généralisée de produire, transformer et diffuser des contenus à grande échelle a abaissé les barrières techniques et économiques d'accès à l'espace public numérique, modifiant les dynamiques de circulation de l'information.

Dans la poursuite de la structuration de l'écosystème médiatique traditionnel, la production, la diffusion et la rentabilisation de l'information par les services numériques s'inscrivent toujours plus dans un cadre où les logiques publicitaires, les abonnements et la captation de l'attention conditionnent la viabilité des médias. Ces modèles reposent largement sur des mécanismes automatisés de recommandation et de ciblage, propres à l'économie des plateformes. Ils favorisent souvent la viralité au détriment de la fiabilité et de la hiérarchisation éditoriale, et peuvent propulser certains contenus sans considération suffisante pour leur source ou leur véracité.

L'immédiateté des réactions permises par ce modèle, combinée à l'importance fondamentale de la liberté d'expression en démocratie, a déplacé une part croissante du débat public vers les réseaux sociaux dont la plupart sont opérés par des entreprises établies hors du territoire national et européen et soumises à des logiques économiques, voire idéologiques, propres. Parallèlement, on observe une érosion continue de la viabilité économique et de la capacité d'enquête des médias traditionnels.

Cette évolution des modes de consommation de l'information fait peser un risque systémique sur la sincérité du débat public : un petit nombre d'acteurs privés régit désormais le cœur de notre infrastructure conversationnelle selon des logiques susceptibles, à certains égards, de nourrir le débat démocratique, mais fondamentalement extérieures à sa raison d'être.

Dans ce contexte, les actions de manipulation ne visent plus seulement à convaincre, mais aussi à saturer l'attention, à déplacer les cadrages, à fragiliser les repères communs, à semer la confusion et à désorganiser les conditions d'un débat public apaisé.

UN DÉBAT PUBLIC SOUMIS À TROIS PRESSIONS

Dans ce contexte de profondes mutations du paysage informationnel, **notre débat public numérique se trouve exposé à un nombre croissant de vulnérabilités,** sous l'influence de trois pressions distinctes : stratégique, systémique et narrative.

PRESSION STRATÉGIQUE : L'INGÉRENCE COMME OUTIL DE PUISSANCE

Tout d'abord, notre espace informationnel est soumis à une pression stratégique croissante, à la faveur d'un contexte international dégradé, facilitant l'émergence d'une conflictualité numérique globale.

Caractérisé par la libre circulation des idées et un accès ouvert aux plateformes de diffusion, cet espace est ainsi devenu le théâtre privilégié de confrontations hybrides où plusieurs compétiteurs étatiques étrangers ont fait de la manipulation de l'information un outil stratégique à part entière, articulé à leurs objectifs diplomatiques, économiques ou de sécurité. En effet, les acteurs étrangers tirent profit de ce contexte pour tenter d'interférer dans notre débat public, d'altérer la perception collective et de peser sur les processus décisionnels.

Ces stratégies visent à semer la confusion, à polariser la société, et, *in fine*, à éroder la confiance du public dans les institutions démocratiques et les médias. Cette tendance est marquée en particulier par la persistance et la sophistication grandissante de modes opératoires informationnels étrangers, qui déploient des dispositifs complexes, leur permettant à la fois de mener des actions planifiées sur le temps long, mais également d'agir opportunément à la faveur de l'actualité. À cet égard, le mode opératoire informationnel *RRN/Doppelgänger,* usurpe l'identité de médias légitimes pour renforcer la crédibilité perçue des messages et fragiliser la confiance dans l'information. Elle se caractérise également par des stratégies informationnelles assumées et désinhibées de la part de compétiteurs étrangers, qui exploitent de manière coordonnée une palette de leviers numériques au service d'une diplomatie publique offensive visant directement les sociétés civiles. En particulier, le débat public numérique autour des conflits en cours (en Ukraine ou entre Israël et le Hamas notamment) est régulièrement exploité par les acteurs de la menace pour accentuer les divisions au sein des sociétés occidentales.

L'acteur russe a par exemple pour objectif principal de saper le soutien occidental à la guerre en Ukraine, tout en déstabilisant des États d'Europe (dont la France), notamment en période électorale. Cet objectif est particulièrement incarné par le réseau appelé *Storm-1516*[1], actif depuis le mois d'août 2023 et très probablement conduit par un service de renseignement russe. Ayant exécuté plus de 150 opérations informationnelles en deux ans, *Storm-1516* a pour principales caractéristiques de produire et diffuser de manière coordonnée de faux contenus audiovisuels, parfois modifiés par une intelligence artificielle, visant à porter atteinte à l'image de ses cibles, dont la France.

S'appuyant sur une doctrine et des moyens structurés, la stratégie informationnelle de la République populaire de Chine est principalement destinée à promouvoir l'image de Pékin auprès des audiences étrangères. À cette fin, des acteurs pro-Parti communiste chinois ont conduit une campagne visant le Rafale de Dassault Aviation lors du conflit récent entre l'Inde et le Pakistan. Elle reposait sur la diffusion de faux contenus, l'usage de comptes non authentiques et une amplification coordonnée des interactions en ligne afin d'altérer la réputation de ce système d'armes à l'export.

À l'été 2023, dans le contexte du conflit avec l'Arménie dans le Haut-Karabagh, l'Azerbaïdjan a déployé une stratégie d'ingérence agressive contre la souveraineté de la France dans ses territoires ultra-marins et en Corse, par le biais de l'amplification des mouvements et idées indépendantistes. Ces manœuvres

[1] Storm-1516 désigne un mode opératoire informationnel (MOI) attribué à des acteurs russes, actif au moins depuis août 2023, regroupant plusieurs dizaines d'opérations informationnelles numériques coordonnées visant à diffuser des narratifs faux ou trompeurs auprès d'audiences occidentales, notamment afin de décrédibiliser des gouvernements (Ukraine, États européens) ou de cibler des processus électoraux et des personnalités politiques.

se sont appuyées sur un groupe spécialement créé à cet effet, le BAKU INITIATIVE GRUP (BIG), ainsi que sur une activité numérique inauthentique ayant notamment visé la Nouvelle-Calédonie – en particulier via l'utilisation de faux comptes, la création de visuels trompeurs et de l'amplification artificielle de ces contenus.

Les démocraties européennes font face à un défi majeur : protéger un débat public ouvert et respectueux de la liberté d'expression de chacun. Cette ouverture est exploitée par des acteurs hostiles. L'enjeu est de protéger nos concitoyens des tentatives de manipulation de l'information en renforçant notre capacité de détection et de réponse, dont d'attribution lorsque cela est possible, tout en continuant à bâtir notre résilience sociétale à travers une mobilisation collective.

PRESSION SYSTÉMIQUE : PLATEFORMES, ÉCONOMIE DE L'ATTENTION ET IA

Par ailleurs, notre espace informationnel numérique est soumis à une pression systémique accrue, exercée par les mutations du paysage numérique lui-même. Cette pression systémique résulte de deux transformations conjointes : la reconfiguration des circuits d'information autour des plateformes et l'intégration rapide de l'IA dans la production et la distribution des contenus.

D'une part, l'évolution du paysage informationnel lui-même, qui voit l'émergence d'un nouvel écosystème numérique de l'information, caractérisé par la place prépondérante des réseaux sociaux, dont certains sont désormais ouvertement employés par leurs dirigeants à des fins politiques, le rôle croissant des influenceurs et l'expansion de l'offre de médias alternatifs d'opinion. Ces évolutions contribuent à éroder encore davantage la consommation des médias traditionnels, et tendent à brouiller la distinction entre une information factuelle et une opinion. Notamment, de très nombreux sites *web* inauthentiques d'information, administrés par des sociétés étrangères de communication numérique liées aux intérêts chinois ou russes, publient en masse des articles, traduits en langue française à l'aide de l'intelligence artificielle et tentent de se positionner dans le paysage numérique français en se présentant comme des médias français officiels.

D'autre part, l'essor de l'intelligence artificielle redéfinit radicalement les usages numériques. Il entraîne une recomposition profonde de l'économie de l'attention, et plus précisément, de la manière dont l'information est produite, distribuée, consommée et monétisée. L'IA agit ainsi en accélérateur d'une transformation profonde du pouvoir et de la valeur dans le paysage numérique : compétition des grandes plateformes, qui tentent de maintenir leur avantage compétitif en devenant des portes d'entrée vers l'IA ; émergence de nouveaux acteurs et modèles économiques ; impact sur les éditeurs traditionnels, contraints de s'adapter dans un environnement où leur visibilité et leurs canaux traditionnels de diffusion sont remis en cause. Ainsi, l'entreprise russe Social Design Agency, opérant une partie des opérations d'ingérence pro-Kremlin, a un recours à l'IA essentiellement centré sur la dissémination de contenus et la protection de ses bots.

En outre, en facilitant la création et la dissémination à grande échelle de contenus synthétiques hyperréalistes – qu'il s'agisse d'images, de vidéos, de sons ou de textes – la prolifération de l'IA fait ainsi légitimement craindre une élévation structurelle du niveau de menace liée aux ingérences numériques étrangères, tant en termes de nouveaux vecteurs que de nouvelles vulnérabilités. Au-delà, une attention spécifique doit être portée à l'utilisation de l'IA à des fins d'amplification de biais algorithmiques cachés, ainsi qu'à la possibilité que les modèles d'IA eux-mêmes soient altérés dès leur phase de construction par des opérations de manipulation de l'information.

PRESSION NARRATIVE : INSTRUMENTALISATION DE THÈMES POLARISANTS

Enfin, notre espace informationnel est soumis à une pression narrative désinhibée, marquée par l'arsenalisation de thématiques puissantes, comme celle de la liberté d'expression.

Une vision absolutiste de la liberté d'expression telle que conçue par certains courants conservateurs

aux Etats-Unis est délibérément introduite dans le débat public européen.[2] L'instrumentalisation de cette thématique est aussi reprise opportunément par les plateformes en ligne, permettant d'entretenir une conception trompeuse, voire erronée, des objectifs de la réglementation numérique européenne (DSA).

En complément, la destruction du dispositif américain d'aide au développement et de soutien à la société civile marque une rupture majeure, en déstabilisant un système de soutien à l'intégrité de l'information établi de longue date.

Tandis que dans les années 2010, ces dynamiques se sont concentrées sur les périodes électorales, elles s'étendent désormais à tous les champs du débat public. Elles visent à polariser l'opinion, saper la cohésion sociale, miner la confiance dans les médias traditionnels et rompre le lien entre citoyens et institutions – jusqu'à générer des troubles à l'ordre public.

Une attention particulière doit également être portée aux territoires ultramarins, qui présentent des vulnérabilités spécifiques dans le champ informationnel. Par leur situation géographique et leur histoire, ces territoires peuvent faire l'objet de campagnes informationnelles ciblées. Au-delà de la détection, la réponse suppose une capacité de proximité : relais institutionnels, médias locaux, acteurs éducatifs et associatifs, afin de limiter la propagation de récits hostiles et de renforcer la confiance dans les vecteurs de médiation (médias, expertise et institutions).

[2] La stratégie nationale de sécurité américaine formule explicitement la posture suivante : « *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, Novembre 2025, p. 26).*

FAIRE FACE AUX VULNÉRABILITÉS DU DÉBAT PUBLIC

POURQUOI CES MANŒUVRES TROUVENT-ELLES UN TERRAIN FAVORABLE ?

L'efficacité des opérations de manipulation de l'information résulte moins de la force intrinsèque des messages que de leur capacité à exploiter des vulnérabilités préexistantes des sociétés visées. Elles relèvent à la fois d'une vulnérabilité structurelle propre aux démocraties ouvertes et de vulnérabilités endogènes, sociales et culturelles.

Les démocraties reposent sur des principes – liberté d'expression, pluralisme, transparence, État de droit – **qui fondent leur légitimité mais peuvent être exploités dans une logique d'asymétrie**. Des acteurs hostiles peuvent agir rapidement, à coût limité et sous le seuil de l'illégalité, là où la puissance publique est tenue par des exigences de proportionnalité, de garanties procédurales et de contrôle démocratique.

Ces opérations exploitent également des fragilités sociales, économiques, culturelles et civiques. Elles s'appuient sur des fractures existantes pour transformer la nature du débat public, polariser les échanges et affaiblir les médiations que constituent les médias, l'expertise et les institutions. Les séquences de crise ou de tension politique tendent à amplifier ces dynamiques, en renforçant simultanément les inégalités et la défiance.

Plusieurs familles de vulnérabilités structurent ainsi l'environnement informationnel. La porosité aux récits manipulatoires est accrue dans les contextes de précarité, d'exclusion et de fragilisation du lien social. La fragilisation économique des médias et la concentration de la visibilité sur un nombre limité d'intermédiaires affaiblissent les médiations informationnelles et les repères partagés. L'essor de l'intelligence artificielle accentue ces vulnérabilités par la production massive de contenus synthétiques et l'opacité croissante des mécanismes de recommandation basés sur des algorithmes.

La défiance à l'égard des institutions constitue un multiplicateur de risque : lorsque la parole publique est systématiquement contestée, l'espace informationnel devient plus réceptif aux récits polarisants et aux entreprises de déstabilisation.

Ces vulnérabilités concernent également les capacités de réponse des acteurs engagés dans la défense du débat public – institutions, médias, société civile, acteurs éducatifs et économiques – dont l'action s'inscrit dans un environnement de plus en plus contraint et fragmenté.

Enfin, l'ambiguïté perçue du rôle de l'État dans l'espace informationnel peut elle-même devenir un facteur de vulnérabilité. Lorsque ses finalités, ses limites et ses garanties ne sont pas clairement identifiées, l'action publique peut nourrir la défiance qu'elle cherche à contenir.

COMMENT ENVISAGER LES EFFETS DE CES MANŒUVRES ?

Les effets des opérations de manipulation de l'information sont difficiles à mesurer avec précision. Ils résultent d'interactions complexes entre exposition aux contenus, mécanismes de recommandation, structures sociales et contexte politique. Les indicateurs disponibles (portée, engagement, viralité) décrivent imparfaitement l'impact réel sur les représentations, les comportements et les décisions collectives. Ces opérations n'agissent généralement pas comme une cause unique, mais comme un facteur d'amplification de tensions déjà présentes.

L'incertitude de la mesure ne signifie pas l'absence d'effet. Ces opérations visent rarement à convertir massivement ; elles cherchent plutôt à produire des effets diffus et cumulatifs : accroissement du bruit informationnel, saturation de l'attention, instillation du doute, affaiblissement de la confiance dans les médias, l'expertise et les institutions, et polarisation par amplification sélective des controverses. Elles peuvent ainsi dégrader progressivement les conditions d'un débat public fondé sur des repères partagés,

sans événement déclencheur identifiable.

Un constat demeure : si ces opérations sont répétées, industrialisées et adaptées en continu, c'est qu'elles répondent à une logique d'efficacité. Les acteurs hostiles investissent dans des dispositifs d'ingérence et d'automatisation, mesurent les réactions, ajustent leurs récits et réutilisent leurs méthodes. La manipulation informationnelle constitue pour eux un levier peu coûteux, flexible et exploitable dans des environnements ouverts.

L'action publique relève donc d'une logique de gestion du risque. Elle doit réduire des vulnérabilités établies, même lorsque l'effet exact d'une campagne ne peut être démontré a posteriori. Exiger une preuve exhaustive avant d'agir créerait une asymétrie durable au bénéfice des adversaires.

Cette logique de gestion du risque implique un cadrage précis du périmètre d'intervention publique.

UN PÉRIMÈTRE D'ACTION PUBLIQUE CIBLÉ

Le dispositif national de lutte contre les manipulations de l'information repose sur un principe démocratique clair : il n'a ni vocation ni mandat pour qualifier les dynamiques nationales. Son champ d'intervention porte sur la détection de manœuvres techniques de manipulation et d'opérations coordonnées impliquant une origine étrangère, dans une logique de sécurité nationale.

Ce choix de construction – fondé sur les garanties démocratiques et sur des critères techniques objectivables – concentre les moyens sur l'amplification artificielle, l'automatisation et la coordination inauthentique. Il protège le pluralisme interne en dissociant l'analyse des procédés de manipulation de toute appréciation des opinions, des acteurs ou des mouvements.

PROJECTIONS À L'HORIZON 2030

Se projeter à l'horizon 2030 est nécessaire, mais incertain. Les transformations technologiques, économiques et informationnelles ne progressent plus par étapes : elles s'accélèrent et se combinent avec des effets difficiles à anticiper. Elles ne concernent plus seulement de nouveaux outils ou usages : elles changent en profondeur la façon dont l'information est produite, diffusée et reçue par le public, et, avec elles, les modes de formation des opinions et du débat collectif.

Il ne s'agit pas d'une rupture brutale ou d'un scénario extrême. Plusieurs de ces dynamiques sont déjà visibles alors que d'autres prolongent des tendances établies. L'enjeu des prochaines années tient moins à leur apparition qu'à leur généralisation et à leur combinaison durable dans les usages quotidiens des services numériques.

Les opérations de manipulation de l'information impliquant des acteurs étrangers évolueront vraisemblablement dans cet environnement reconfiguré. Trois dynamiques techniques, déjà observables, structurent cette évolution dans les scénarios dominants à ce stade :

- la capacité à produire des contenus à très grande échelle, souvent à faible coût ;
- l'automatisation croissante de leur diffusion et de leur interaction ;
- et la centralité de systèmes de sélection et de recommandation dont la transparence fait l'objet d'exigences réglementaires croissantes, avec des effets encore inégalement mesurés.

LA BANALISATION DE LA GÉNÉRATION SYNTHÉTIQUE : RISQUE D'UNE POSSIBLE FRAGILISATION DE LA PREUVE

Depuis plusieurs années déjà, des contenus générés artificiellement – textes, images, sons ou vidéos – **circulent massivement en ligne**. À l'horizon 2030, cette production pourrait devenir entièrement banale, intégrée aux outils du quotidien et aux gestes ordinaires de communication et de recherche d'information.

La nouveauté ne tient pas seulement au volume de contenus produits, mais aussi à leurs effets cumulatifs sur la confiance. Lorsque des traces numériques peuvent être produites instantanément et en nombre, leur valeur probante tend à s'affaiblir. Ce qui faisait auparavant preuve comme élément visuel ou sonore isolé devient plus fragile et plus facilement contestable. Des mécanismes techniques de certification, de traçabilité et de signature des contenus émergent toutefois en parallèle (*watermarking* par exemple), sans garantie à ce stade de généralisation.

Dans ce contexte, la frontière entre information, commentaire, interprétation et manipulation devient moins lisible. Lorsqu'elle se combine avec des capacités de diffusion coordonnées, cette évolution accroît potentiellement de manière mécanique l'efficacité d'opérations de manipulation de l'information d'origine étrangère reposant sur la diffusion massive et délibérée de contenus trompeurs, en réduisant la capacité des publics à discriminer une production authentique d'une fabrication artificielle.

L'HYPERPERSONNALISATION ALGORITHMIQUE : VERS UNE RÉALITÉ DE PLUS EN PLUS FRAGMENTÉE

Cette banalisation s'accompagne d'une personnalisation accrue de l'information. Les systèmes de sélection et de recommandation pourraient évoluer vers une différenciation de plus en plus individualisée, intégrant préférences et comportements dans certaines catégories d'usages et de plateformes.

La polarisation ne résulterait alors plus seulement des désaccords d'opinion, mais du fait que les individus n'accèdent plus aux mêmes sujets ou aux mêmes récits, avec des mises en perspective différentes. Cette fragmentation crée un terrain favorable aux stratégies d'ingérence, qui peuvent cibler

des publics segmentés, adapter les messages et exploiter des clivages existants.

L'AUTOMATISATION DES INTERACTIONS : UN DÉBAT PUBLIC SOUS CONTRAINTE D'ATTENTION

L'automatisation des interactions a déjà franchi un seuil. Des dispositifs, notamment des agents IA ou des modèles agentiques, capables de produire, relayer et amplifier des prises de parole commencent à participer aux échanges en ligne dans certains environnements. À mesure qu'ils gagnent en fluidité et en autonomie, ils peuvent devenir des composantes ordinaires de l'espace public dans certains segments de plateformes, sans être toujours identifiables comme telles malgré le développement d'outils de détection et de labellisation automatisée.

L'enjeu ne consiste alors plus seulement à convaincre, mais à imposer une dynamique d'attention : capter l'attention, maintenir un sujet au premier plan et, *in fine*, saturer les capacités d'échange. Le débat public peut ainsi être moins structuré par la qualité des arguments que par la capacité à orienter ou disperser l'attention collective. Ces logiques s'accordent avec des modes opératoires d'ingérence fondés sur la diffusion artificielle et coordonnée de contenus, visant moins la persuasion directe que la perturbation durable du débat public.

LES NOUVEAUX INTERMÉDIAIRES NUMÉRIQUES : UNE POSSIBLE TRANSFORMATION DE L'ACCÈS À L'INFORMATION

L'accès à l'information s'étend vers de nouveaux intermédiaires : interfaces conversationnelles, services intégrés aux outils du quotidien, systèmes capables de formuler directement des réponses. Ces dispositifs ne renvoient plus seulement vers des sources : ils sélectionnent, reformulent et hiérarchisent les contenus.

La vulnérabilité ne se situe donc plus uniquement au niveau de la production de l'information, mais dans les critères de sélection et de présentation, qui conditionnent en partie la crédibilité perçue. Souvent peu visibles, ces mécanismes influencent la compréhension et la hiérarchisation des sujets, selon des architectures et des paramètres variables selon les services, sans toujours pouvoir être explicités. Ils peuvent ainsi constituer des cibles pour des opérations informationnelles étrangères cherchant à agir indirectement sur la formation des opinions.

NOUVEAUX MODES DE CONSOMMATION DE L'INFORMATION : DES STRATÉGIES DE PLUS EN PLUS ADAPTÉES À L'IA

À mesure que l'intelligence artificielle devient une interface d'accès à l'information – moteurs génératifs, assistants conversationnels, outils de synthèse – les stratégies d'ingérence informationnelle sont susceptibles d'évoluer. Elles pourraient viser non plus seulement les publics, mais les systèmes chargés de produire, d'organiser et de reformuler l'information.

Dans un environnement où la valeur informationnelle repose de plus en plus sur les données – corpus d'entraînement, contenus indexés, signaux d'ajustement des modèles – l'action d'ingérence peut s'exercer en amont, par une intervention directe ou indirecte sur ces ensembles de données, plus facilement sur les couches d'indexation et de recherche dans des environnements ouverts, que sur les modèles fondamentaux eux-mêmes dont les corpus d'entraînement devraient, en théorie, être plus filtrés et préparés. Cette dépendance accroît la sensibilité des écosystèmes linguistiques moins volumineux. L'espace numérique francophone, moins dense que l'espace anglophone, peut à ce titre présenter une vulnérabilité particulière aux déséquilibres ou aux altérations ciblées des corpus.

Ces approches correspondent à des modes opératoires adverses : action intentionnelle, outillée, automatisable et compatible avec des interventions à grande échelle. Elles peuvent prendre la forme d'injections de contenus orientés dans des espaces fortement explorés par les systèmes automatisés, d'optimisations destinées aux moteurs génératifs (techniques proches du référencement adapté aux systèmes IA), ou d'altérations de jeux de données de référence lorsqu'ils sont ouverts, contributifs ou

insuffisamment contrôlés. L'objectif n'est plus seulement la visibilité d'un message, mais sa probabilité d'intégration dans des synthèses automatiques ou dans les classements implicites de crédibilité.

Ces stratégies présentent pour leurs promoteurs plusieurs caractéristiques : coût limité, attribution difficile, effets différés et capacité d'action sous les seuils de détection usuels. Elles s'inscrivent dans le temps long et visent des effets structurels plutôt que des impacts ponctuels.

TROIS PRINCIPES DIRECTEURS POUR GUIDER L'ACTION PUBLIQUE

Afin de pleinement respecter les exigences précédemment énoncées, la présente stratégie nationale de lutte contre les manipulations de l'information repose sur trois principes fondamentaux : l'ouverture, l'action en réseau et l'intégration. Ces principes visent à articuler les réponses institutionnelles, à élargir le périmètre des acteurs impliqués et à renforcer la résilience de la société dans son ensemble face aux menaces informationnelles, dans le strict respect des principes démocratiques constitutionnels, européens et internationaux.

L'OUVERTURE

Contrairement à d'autres champs de la sécurité nationale fondés sur la confidentialité, la lutte contre les manipulations de l'information s'appuie, dans une large mesure, sur des méthodes et des ressources publiquement accessibles. Cette orientation marque un changement important de paradigme : elle privilégie la transparence, la vérifiabilité, et la mobilisation de l'ensemble des parties prenantes.

L'action de VIGINUM illustre cette approche. Le service fonde son activité sur des données publiquement accessibles, publie ses analyses et rend accessibles une partie de ses méthodes et de ses outils. Ce choix stratégique, qui sera renforcé et rendu régulier, vise à permettre la reproduction, la vérification, la contestation et la contribution par des acteurs tiers. Il ne va pas sans questions – notamment sur les risques de valorisation involontaire des menaces ou d'exposition des capacités nationales – mais il est tranché avec discernement, au cas par cas.

Cette logique d'ouverture et de transparence est un levier de renforcement démocratique : en donnant au public les moyens de comprendre les mécanismes de manipulation, elle réduit leur efficacité. Une campagne de manipulation informationnelle ne peut opérer durablement sans opacité. La transparence devient ainsi un outil préventif autant que curatif, contribuant à une meilleure appropriation citoyenne des enjeux liés à l'ingérence numérique étrangère.

L'ACTION EN RÉSEAU

La lutte contre les manipulations de l'information ne saurait être portée par une entité isolée. Elle repose sur une mobilisation distribuée, s'appuyant sur une logique de coopération entre les administrations, les institutions, les acteurs techniques, les régulateurs, les chercheurs, les médias, les plateformes, la société civile et les citoyens – chacun à son niveau de responsabilité.

Cette coopération a vocation à prendre plusieurs formes détaillées dans la présente stratégie : échanges d'informations, actions conjointes, structuration de dispositifs permanents ou ponctuels. Plusieurs instances nationales illustrent cette dynamique. D'autres formats de coordination existent à des échelles bilatérales, sectorielles ou européennes, comme le Réseau des régulateurs du numérique ou le Comité européen des services numériques, ou bien encore le Système d'alerte rapide européen.

Au sein de l'État, cette logique implique une approche interministérielle par nature : au-delà des services spécialisés en détection ou réponse, toutes les administrations intervenant dans le champ social, sanitaire, éducatif, culturel ou civique doivent pouvoir être mobilisées. L'engagement citoyen, la relation au public et l'éducation aux médias doivent ainsi s'inscrire dans cette dynamique collective.

L'INTÉGRATION

Enfin, la lutte contre la manipulation de l'information exige une approche globale et systémique. Dans un environnement numérique interconnecté, aucun domaine de la vie sociale n'échappe à la circulation des contenus. Les frontières traditionnelles – entre physique et virtuel, national et international, public et privé – tendent à s'effacer au profit de phénomènes transversaux, impliquant une diversité d'acteurs.

La réponse doit être à la hauteur de cette complexité : elle suppose une coordination accrue entre

institutions, une reconnaissance mutuelle des compétences et une capacité à mobiliser toutes les forces vives – administrations, entreprises, laboratoires de recherche, associations et citoyens.

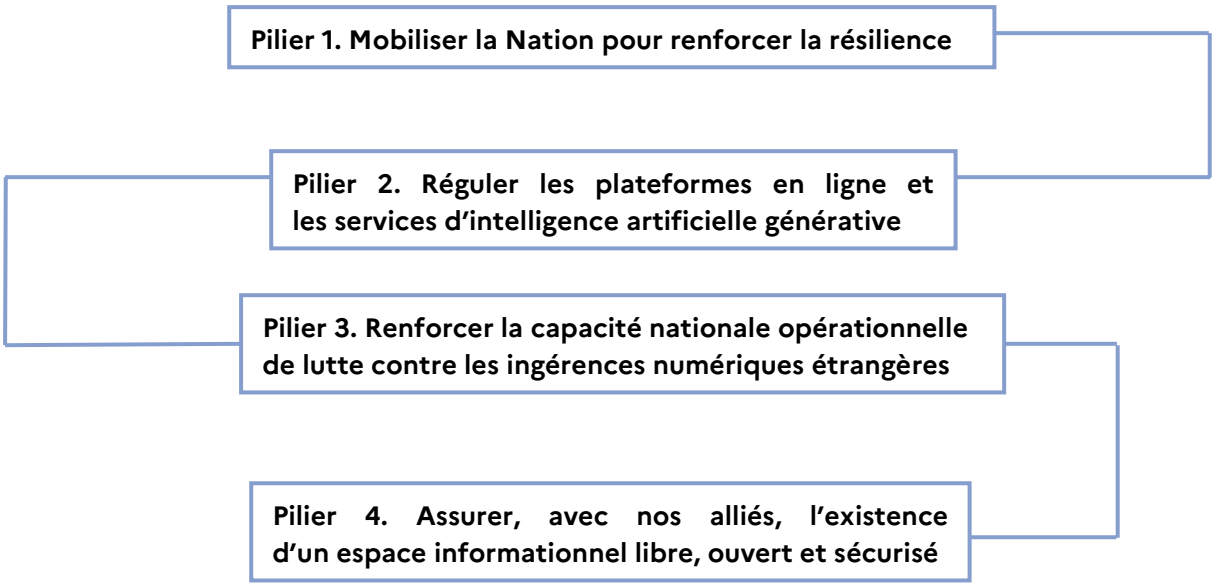
L'intégration renvoie également à une exigence de partage de l'information, dans le respect des impératifs de sécurité. Le renforcement de la confiance mutuelle entre acteurs publics et privés repose sur la circulation maîtrisée de ce qui est su, de ce qui est en cours d'évaluation, et de ce qui demeure encore incertain.

Par cette approche, **chaque entité, chaque citoyen peut devenir un acteur de la résilience informationnelle**, en participant à la détection, à la compréhension ou à la remédiation des tentatives de manipulation.

Ces trois principes – ouverture, action en réseau, intégration – **constituent les fondements opérationnels de la présente stratégie**. Ils doivent permettre de capitaliser sur les dynamiques déjà engagées, tout en assurant une montée en puissance collective et une opérationnalisation de nature à répondre à l'intensité croissante des enjeux relatifs à la lutte contre les ingérences étrangères. Ils guideront l'action dans les années à venir, y compris face aux menaces non encore identifiées, dans un environnement informationnel en constante mutation et serviront de socle aux objectifs stratégiques définis dans la suite du document.

UNE STRATÉGIE DÉCLINÉE EN 15 OBJECTIFS STRATÉGIQUES

En déclinaison de la Revue nationale stratégique et dans le prolongement de l'action de l'État en matière de lutte contre les manipulations de l'information, la présente stratégie adopte une approche structurée, articulée autour de quatre grands piliers :



Déclinée en 15 objectifs stratégiques, cette stratégie globale, coordonnée et évolutive vise à consolider l'avance de la France dans la préservation de l'intégrité du débat public et de prolonger ses efforts de résilience démocratique face aux manipulations de l'information. Elle privilégie une logique de cohérence stratégique plutôt qu'une recherche d'exhaustivité, afin de concentrer l'action publique sur les leviers les plus efficaces et mobilisables.

Plutôt que de rechercher une complétude illusoire à travers un inventaire d'actions exhaustif, la stratégie propose des ressorts d'action concrets, des lignes de conduite partagées et des objectifs opérationnels non limitatifs, destinés à orienter l'action publique à court et moyen terme. Elle a pour ambition d'imprégner les démarches des acteurs impliqués, qu'ils soient étatiques ou non, d'une philosophie d'action claire, partagée et évolutive**.**

Face à l'ampleur de la menace, l'enjeu central identifié de la stratégie est la constitution et l'animation d'un collectif à l'échelle du pays, et au-delà, dans une logique de réponse concertée à l'échelle internationale. Cela induit :

- **d'impliquer l'ensemble de la population** dans la compréhension des phénomènes de manipulation ;
- **de partager largement l'information utile** à la prévention et à la détection de ces phénomènes ;
- **de renforcer la capacité d'action** des entités publiques et des acteurs de terrain ;
- **de mutualiser les ressources opérationnelles disponibles** afin d'assurer une réponse coordonnée et efficace.

Au cœur de cette stratégie se trouve l'ambition de dépasser la simple lutte contre les manipulations de l'information pour construire une société capable de maintenir la confiance et des repères communs. Chaque citoyen, acteur public ou privé, doit disposer des moyens de s'informer de manière éclairée, de comprendre les mécanismes d'ingérence et de contribuer activement au débat démocratique. Cette ambition s'articule avec d'autres leviers – services numériques, éducation, culture, aménagement du territoire – qui, bien que hors du périmètre strict ici visé, soutiennent la consolidation de cette confiance.

PILIER

01

Mobiliser la Nation pour renforcer sa résilience

Forger une société résiliente en faisant de chaque citoyen un acteur éclairé contre la manipulation de l'information, grâce à un parcours d'engagement unique et un réseau unissant citoyens, institutions et acteurs clés de la société civile.

Face aux manipulations de l'information et aux ingérences numériques étrangères, un enjeu stratégique de premier ordre est de **renforcer la résilience de la société** dans son ensemble, en agissant sur les **facteurs cognitifs, sociaux, éducatifs et culturels** que ces manipulations exploitent.

Cela suppose de bâtir un **socle de compétences et de connaissances critiques** accessible à tous, sur les modes opératoires et techniques que des acteurs étrangers utilisent pour s'ingérer dans notre débat numérique et sur les risques spécifiques posés par l'utilisation de certaines technologies numériques (IA générative, algorithmes de recommandation, etc.), de créer des **parcours d'engagement et de spécialisation** autour des enjeux informationnels, et de mobiliser les **leviers éducatifs, associatifs, scientifiques et citoyens** sur l'ensemble du territoire.

La première condition de cette résilience est la constitution d'une capacité nationale d'expertise, apte à détecter, caractériser et comprendre les opérations de manipulation de l'information (OS1). À cette fin, la France porte une approche fédérative autour d'une Académie de la lutte contre les manipulations de l'information, placée au sein du service VIGINUM. Organisée de manière distribuée, cette structure s'appuiera sur les acteurs existants pour former un réseau de référents, fournir les compétences clés, transférer des ressources techniques et favoriser l'émergence de référents territoriaux. Ce réseau constituera la colonne vertébrale opérationnelle de la stratégie française de résilience démocratique.

En parallèle, la stratégie nationale vise à déployer une filière complète de formation, de sensibilisation et de recherche, adossée à l'École, à l'enseignement supérieur et au monde académique (**OS2**). Cette filière intégrera progressivement les enjeux de manipulation de l'information dans les cursus scolaires, proposera des modules de formation à destination des enseignants et chercheurs, et soutiendra des projets de recherche interdisciplinaires à fort impact. L'objectif est de **construire un écosystème de connaissance durable**, capable d'éclairer l'action publique et de renforcer l'esprit critique dès le plus jeune âge.

Au-delà du système éducatif, l'État mobilisera également les dispositifs d'engagement civique pour former une jeunesse active dans la défense du débat public (**OS3**). **La Journée Défense et Citoyenneté (JDC), le Service militaire volontaire ainsi que le Service et la Réserve civiques** seront autant d'occasion de diffusion de contenus relatifs à la lutte contre les manipulations de l'information. La réserve citoyenne du numérique sera mobilisée pour former et porter les personnes souhaitant agir au service de la lutte contre les manipulations de l'information. Des modules pédagogiques et des missions dédiées y seront introduits pour renforcer l'engagement et ouvrir des **passerelles vers les réserves citoyennes**.

Enfin, la stratégie s'appuie sur la diffusion à large échelle d'une culture citoyenne de protection face aux manipulations de l'information (OS4). Cette dynamique repose sur des formats souples et participatifs (ateliers, débats, forums), portés localement par un **réseau de personnes formées**, issues de l'éducation aux médias et à l'information, de l'éducation populaire, du monde associatif ou de l'Académie de la lutte contre la manipulation de l'information.

Des initiatives populaires ou étatiques déjà implantées nationalement pourront servir de socle pour structurer des espaces d'échange grand public sur les manipulations informationnelles. L'objectif est de **créer une culture collective au sein de l'ensemble de la population**, dans une logique de proximité, d'ouverture et de prévention.

OBJECTIF STRATÉGIQUE 1. PORTER UNE CAPACITÉ COLLECTIVE DE LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION

La capacité collective de lutte contre les manipulations de l'information exige de former des acteurs capables de mobiliser leurs connaissances de manière intégrée aux structures professionnelles et sociales participant de près ou de loin au fonctionnement de notre environnement informationnel.

Une première exigence est d'assurer la fiabilité de l'environnement informationnel national au sens large, qu'il soit numérique ou non. Pour cela, il importe de mettre en partage les éléments de compréhension et d'analyse nécessaires, qu'ils ressortent de la recherche, de sphères civiles ou de l'État, en priorité avec les personnes qui disposent d'un rôle particulier dans le fonctionnement de notre espace informationnel commun.

Au long cours, ces connaissances, savoir-faire et réflexes doivent pouvoir être intégrés dans l'ensemble des structures déterminantes pour le fonctionnement du pays. Cela requiert des adaptations organisationnelles mais aussi l'existence d'une nouvelle génération de professionnels hautement qualifiés dans des domaines tels que la veille stratégique, l'analyse des réseaux sociaux, l'évaluation des manipulations algorithmiques, l'utilisation malveillante des systèmes d'IA, les mécanismes techniques de réponse, l'investigation numérique ou encore la compréhension technique des dynamiques informationnelles.

Ces savoir-faire, pourtant déterminants, ne font pas aujourd'hui l'objet d'une structuration nationale à grande échelle. Ce champ souffre dès lors d'une pénurie de compétences, accentuée par une sous-représentation sociale et de genres, caractéristique plus large du secteur numérique, et par un manque d'alignement entre les profils formés et les besoins réels du terrain. Dans ce contexte, il est indispensable que la France agisse à court et long terme.

À court terme, il importe de fournir à l'ensemble des décideurs locaux et nationaux, aux cadres de l'administration ainsi qu'aux directeurs des médias et journalistes, une information claire sur les mécanismes techniques et technologiques utilisés dans les opérations de manipulation de l'information. Les organes de formation professionnels propres à chaque corps professionnel pourront être mobilisés à cette fin.

Cela doit permettre d'aller à l'essentiel de la compréhension non pas seulement d'événements ponctuels mais de mécaniques globales et structurelles dans un contexte où les ingérences étrangères sont de plus en plus nombreuses et tangibles.

Cette communication initiale sera complétée de la communication régulière de bulletins d'informations relatifs aux modalités d'ingérences étrangères détectées dans le champ informationnel ainsi que des éléments généraux de compréhension similaires à ceux déjà diffusés par VIGINUM.

Sur le long terme, il importe d'investir massivement dans le développement de ces expertises, en les intégrant notamment aux cursus de formation existants dans les domaines régaliens, les médias, les sciences sociales et le numérique.

En partenariat avec les collectivités territoriales, les établissements d'enseignement supérieur, les académies, le monde associatif, les médias, les opérateurs publics de formation et les acteurs économiques concernés, l'État développera une politique nationale de formation structurée, à destination d'un public d'acteurs clefs.

Cette approche fédérative permettra de capitaliser sur les ressources existantes tout en valorisant les savoir-faire acquis par de très nombreux acteurs, qu'ils soient nationaux, européens ou internationaux. Un lien sera également opéré avec les apprentissages en matière de cybersécurité.

DONNER UN RÔLE FÉDÉRATIF À L'ACADÉMIE DE LA LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION (ACADÉMIE DE LA LMI)

À l'horizon 2027, la France structurera et déploiera une Académie de la LMI, au sein du service VIGINUM. Elle sera chargée de publier et d'assurer la circulation des socles nécessaires de connaissances techniques, déjà existants pour une très large part, qu'ils portent sur les modalités techniques ou ressorts sociaux, psychologiques ou comportementaux, numériques ou non, des manipulations de l'information. Elle impliquera l'ensemble des acteurs publics compétents et filières de formations déjà dédiées.

Ces connaissances devront avant toute chose porter sur les techniques de manipulation de l'information, ainsi que sur les dynamiques structurelles à long terme, qu'elles soient sociales, psychologiques, ou technologiques, et sur les ressorts qui conduisent à l'adoption de certains comportements.

L'Académie de la LMI assurera trois missions principales :

- **concevoir et partager des ressources pédagogiques** adaptées à chaque public cible (éducation, sensibilisation, formation), à destination des élus, des préfectures, des collectivités territoriales, des administrations publiques, de l'Éducation nationale, des médias, des entreprises, associations et du grand public.
- **former le plus grand nombre, en diffusant** des compétences acquises et d'outils technologiques et en assurant la diffusion d'une culture opérationnelle commune pour faire face aux ingérences numériques étrangères. Ce réseau sera articulé avec les dynamiques de formation en cybersécurité, dans une logique de complémentarité.
- **développer une offre de renforcement capacitaire à l'échelle internationale**, conforme à nos priorités nationales et européennes, destinée aux partenaires étrangers souhaitant se doter de structures similaires à VIGINUM. Cette coopération permettra également à l'Académie d'enrichir ses propres ressources grâce aux contributions méthodologiques ou pédagogiques de ses partenaires.

OBJECTIF STRATÉGIQUE 2. BÂTIR UNE FILIÈRE D'ÉDUCATION ET DE RECHERCHE DEDIÉE À LA RÉSILIENCE INFORMATIONNELLE

Structurer une dynamique cohérente et interdisciplinaire d'éducation transgénérationnelle et de recherche transdisciplinaire pour renforcer durablement la capacité de la société à comprendre, détecter et contrer les manipulations de l'information.

Face à l'ampleur et à la complexité des phénomènes de manipulation de l'information, la France engage une politique publique cohérente, structurée et interdisciplinaire d'éducation à l'information et de recherche sur les dynamiques informationnelles.

Cette stratégie vise à bâtir une filière complète de long terme, allant de la sensibilisation citoyenne transgénérationnelle à la recherche académique de haut niveau, en mobilisant durablement l'ensemble des acteurs concernés : l'École, l'université, la recherche, les médias, la sphère culturelle et la société civile. L'objectif est de **diffuser, à tous les niveaux de la société, les compétences critiques essentielles** à la compréhension, à la détection et à la remédiation des manipulations de l'information, dans une logique de renforcement de la résilience démocratique.

RENFORCER L'ÉDUCATION AUX MÉDIAS ET À L'INFORMATION DANS LE SYSTÈME SCOLAIRE

L'éducation aux médias et à l'information (EMI), dont un des objectifs est de développer l'esprit critique dans le traitement de l'information, et l'intégration des éléments pédagogiques sur les manipulations de l'information dans les enseignements concernés, notamment un enseignement moral et civique (EMC), constituent un levier fondamental de formation des jeunes citoyens. Cette intégration, déjà effective dans les nouveaux programmes applicables progressivement depuis la rentrée 2024, sera encore renforcée dans les différents programmes d'enseignements.

Les partenariats du ministère chargé de l'éducation nationale avec VIGINUM ou l'ARCOM contribueront aux objectifs suivants :

- **la diffusion du parcours MAGISTÈRE d'autoformation à plus grande échelle et le déploiement de formations en académies en appui de ce parcours** ;
- **un renforcement de la diffusion des ressources existantes**, en particulier produites par le CLEMI et valorisées sur le site *éduscol* ;
- **la production de nouvelles ressources** : des ressources pour LUMNI ENSEIGNEMENT en collaboration avec l'INA et FRANCE TV, ainsi que des outils comme l'évolution du projet THE OSINT PROJECT ou la plateforme PIX, dont les usages pédagogiques seront valorisés et démultipliés.

MOBILISER L'OFFRE ACADÉMIQUE ET LES ACTEURS DE L'ENSEIGNEMENT SUPÉRIEUR

Les ministères compétents, notamment ceux chargés de l'Enseignement supérieur ou encore de la Santé, des Familles, de l'Autonomie et des Personnes handicapées[3], seront pleinement mobilisés pour rappeler à ses opérateurs l'importance de prendre en compte la lutte contre les manipulations de l'information et l'éducation critique aux médias et à l'information dans la construction de leurs stratégies de formation. Plusieurs filières préparent aux métiers relevant de l'éducation critique aux médias, de l'information et du journalisme ainsi que du traitement des informations et du renseignement en sources ouvertes (OSINT) et pourront former des experts spécialistes de ces questions. Elles reposent sur les disciplines des sciences de l'information et de la communication, du droit, du numérique et des sciences des données, des sciences cognitives, ou encore de la géopolitique – notamment dans le champ numérique.

Des actions de sensibilisation pourront être proposées aux doctorants dans le cadre de l'enseignement

[3] Voir Stratégie nationale de lutte contre la désinformation en santé

obligatoire à l'intégrité scientifique et aux enseignants-chercheurs nouvellement recrutés. Réciproquement leurs compétences pourront être mobilisées en lien d'ailleurs avec celles de la société dans son ensemble dans une logique de recherche ouverte. Ces actions pourront s'appuyer sur la sensibilisation et la formation déjà structurées et développées dans le réseau des bibliothèques universitaires et des acteurs de formation à l'information scientifique, et s'appuyer sur le réseau des professionnels de l'information scientifiques ainsi que sur les plateformes de diffusion de contenus scientifiques alimentées par les établissements d'enseignement supérieur.

Le sujet sera également pris en compte dans le cadre des enseignements de méthodologie dispensés aux étudiants de licence et master. Une analyse de l'intégration dans ces enseignements existants des contenus dédiés à l'identification des procédés techniques utilisés pour manipuler l'information sera réalisée et des actions de soutien pour renforcer la présence de ces thématiques seront proposées aux établissements. En parallèle, un **réseau des communicants** au sein des établissements d'enseignement supérieur et de recherche sera mis en place pour renforcer les capacités de veille, de partage d'informations et de riposte face aux manipulations de l'information.

Ce réseau facilitera l'accessibilité et la visibilité des travaux et contenus qui éclairent l'actualité, répondent aux attaques informationnelles, mettent en valeur les travaux et projets de recherche, et participent à l'enrichissement du débat public ainsi qu'à la diffusion d'une culture scientifique, à l'attrait et à la démocratisation de la science. Il s'appuiera et se coordonnera notamment avec le travail de lutte contre la désinformation portée par les bibliothèques universitaires et les structures documentaires de l'enseignement supérieur et de la recherche.

SOUTENIR LA RECHERCHE INTERDISCIPLINAIRE SUR LES PHÉNOMÈNES INFORMATIONNELS

L'enjeu principal consiste à identifier avec précision les besoins en recherche, en établissant **un état des lieux complet de l'existant et des manques**, qu'il s'agisse des sphères institutionnelles, académiques ou des filières de recherche, qu'elles soient publiques ou privées. Ce diagnostic permettra de **mobiliser les moyens de financement les plus adaptés** (programmes dédiés ou chaires) pour soutenir des travaux tout en garantissant à la fois la liberté inhérente à la recherche et leur contribution à la compréhension de ces défis sociétaux majeurs.

En première approche, il s'agira d'articuler un **travail en deux volets** : d'une part, conduire des études approfondies sur la reconfiguration de **l'économie de l'information en ligne** et, plus largement, le **paysage informationnel** (modèles d'affaires, architectures techniques, technologies émergentes, chaînes de valeur), en intégrant le **potentiel de transformation majeur de l'IA générative** ; d'autre part, analyser l'**impact des manipulations de l'information**, en termes d'exposition, de réception et de modification des attitudes et comportements, ainsi que les **modes de remédiation** proposés.

OBJECTIF STRATÉGIQUE 3. MOBILISER LES PARCOURS D'ENGAGEMENT CIVIQUE AU SERVICE DE LA PROTECTION DU DÉBAT PUBLIC

Mobiliser les dispositifs d'engagement civique pour sensibiliser les citoyens les plus jeunes, valoriser les compétences acquises et structurer un vivier de citoyens actifs face aux manipulations de l'information.

L'engagement civique constitue un levier stratégique pour sensibiliser, former et mobiliser une génération de citoyens acteurs de la protection du débat public. Pour faire émerger une société résiliente face aux manipulations informationnelles, l'État renforcera et adaptera les **dispositifs d'engagement existants** en y intégrant pleinement les enjeux liés aux ingérences numériques étrangères.

Complémentaire des parcours formalisés d'engagement civique, cette dynamique vise à irriguer l'ensemble du tissu social de formats accessibles à tous. L'objectif est double : permettre à chaque citoyen de mieux comprendre les dynamiques informationnelles qui structurent l'espace public, tout en ouvrant des parcours d'engagement concrets permettant de nourrir le vivier de compétences nécessaires à la défense de nos institutions démocratiques.

INTÉGRER LES ENJEUX DE LA LMI DANS LES DISPOSITIFS EXISTANTS

Plusieurs dispositifs d'engagement volontaire, déjà en place, seront mobilisés pour diffuser à large échelle une **culture citoyenne de vigilance et de résilience informationnelle**.

La **Journée défense et citoyenneté (JDC)** constituera un moment clé pour présenter les enjeux fondamentaux de la lutte contre les ingérences numériques étrangères, conformément aux recommandations du rapport sénatorial de 2024 relatif à la lutte contre les influences étrangères malveillantes intitulé *« Pour une mobilisation de toute la Nation face à la néo-guerre froide »*. Un module synthétique y présentera les mécanismes techniques de manipulation et les bonnes pratiques de vérification.

La Réserve civique et le Service civique, en tant que cadres d'engagement volontaire de plus ou moins longue durée, offriront l'opportunité à de nombreux jeunes de découvrir les métiers liés à l'information et à la protection du débat public. En lien avec les acteurs du secteur (médias, associations, institutions), des **missions spécifiques** seront proposées et valorisées.

Dans cette dynamique, **la réserve citoyenne du numérique** créée par l'article 23 de la loi SREN du 21 mai 2024 devra également être mobilisée afin de nourrir et de porter l'effort collectif en matière de lutte contre la manipulation de l'information. Cette mobilisation pourra se traduire par la diffusion d'informations et d'éléments de compréhension au sein de la population, mais aussi par la participation à des activités de veille, d'analyse et de réponse face aux menaces. Les réservistes bénéficieront d'un accès privilégié aux informations actualisées sur les menaces en cours, leur permettant ainsi de renforcer et de démultiplier la capacité d'action à l'échelle nationale.

CRÉER DES PASSERELLES VERS LES RÉSERVES CITOYENNES ET OPÉRATIONNELLES

Pour pérenniser les compétences acquises et capitaliser sur l'expérience des volontaires, des **passerelles structurées** seront créées vers les **réserves citoyennes et opérationnelles**, permettant d'entretenir l'engagement au-delà des dispositifs initiaux.

OBJECTIF STRATÉGIQUE 4. FAIRE ÉMERGER UNE CULTURE CITOYENNE DE PROTECTION FACE AUX MANIPULATIONS DE L'INFORMATION

Faire émerger une culture citoyenne de protection face aux manipulations de l'information en diffusant à l'échelle nationale des formats de sensibilisation participatifs, portés par un réseau de référents locaux.

Face à des dynamiques informationnelles de plus en plus complexes techniquement et à la multiplication des vecteurs de manipulation, chaque citoyen doit pouvoir accéder aux **compétences nécessaires pour comprendre, analyser et réagir** face à des opérations diverses de manipulation et d'ingérence étrangère. L'objectif est de **favoriser le développement de l'esprit critique**, dans une logique d'**autonomisation et de sensibilisation à même de remplir les fonctions de défense collective**. Cette ambition suppose de **multiplier les formats d'intervention adaptés** (ateliers, débats, conférences, expériences immersives, etc.), en s'appuyant sur des dynamiques locales, participatives et décentralisées, à destination de tous les publics et sur l'ensemble du territoire.

CAPITALISER SUR LES INITIATIVES PUBLIQUES, POPULAIRES ET ISSUES DE LA SOCIÉTÉ CIVILE

Face aux enjeux croissants de manipulation de l'information, **de nombreuses initiatives, allant de l'éducation populaire aux espaces de débat citoyen, œuvrent déjà à outiller et sensibiliser l'ensemble de la population**.

L'éducation populaire joue un rôle clé dans la diffusion d'outils, formations et informations pour comprendre et se protéger des manipulations de l'information. Non seulement elle intervient sur les questions numériques mais elle couvre aussi de nombreux savoirs fondamentaux – scientifiques, historiques, ou encore civiques – tous nécessaires à la résilience de la population. Plus récemment, l'initiative Café IA a commencé à offrir des espaces d'échanges ouverts à tous pour échanger sur nos relations à l'IA, s'orienter et expérimenter.

Sur le plan des ressources, des structures comme le CLEMI constituent une illustration de formes de mobilisation déjà très implantées et qui contribuent à sensibiliser aux enjeux informationnels.

Il convient également d'apporter un soutien particulier à la contribution et à la valorisation de ressources telles que Wikipédia, qui bénéficient d'un important capital de confiance et jouent un rôle central dans les usages de vérification de l'information par les Français, sur quelque forme de de savoir que ce soit, leur fiabilité et leur qualité reposant directement sur l'engagement et l'étendue de leurs communautés.

La stratégie nationale appuiera ces dynamiques plurielles en mettant à disposition, regroupant, rassemblant ou consolidant selon les besoins, des ressources pédagogiques, conçues en lien avec les acteurs de l'éducation aux médias et à l'information, tout comme de l'éducation populaire et civique en général, et en **v**alorisant les initiatives locales existantes**.**

DÉPLOYER, FÉDÉRER ET ANIMER UN RÉSEAU D'ACTEURS ET DE MÉDIATEURS

L'adhésion à des démarches de médiation numérique, d'éducation populaire ou du type Café IA repose sur l'existence d'un réseau national d'acteurs de très grande proximité, capables d'animer au plus près des citoyens des espaces mêlant échanges et diffusion de savoirs. Les acteurs que sont les médiateurs numériques revêtent une richesse d'autant plus particulière qu'ils permettent de **maintenir un lien avec les personnes les plus isolées et potentiellement en situation de vulnérabilité**. Leur rassemblement en un **réseau animé, nourri et coordonné** permettra d'assurer un travail de proximité spécifique.

En matière de lutte contre la manipulation de l'information, **ce réseau sera enrichi de formateurs et animateurs de l'éducation aux médias et à l'information** dans le cadre de l'éducation populaire, d'acteurs du monde associatif et médiatique impliqués dans la formation citoyenne, ainsi que de personnes formées via l'Académie de la LMI, les filières éducatives et universitaires, les parcours d'engagement civique, etc.

Les membres de ce réseau seront outillés et accompagnés dans la durée grâce à un dispositif de **formation continue**, alimentée par les ressources pédagogiques de partenaires scientifiques ou institutionnels co-produites avec VIGINUM.

Un **canal d'information** garantira l'actualisation des connaissances et la diffusion rapide des signaux faibles. Ce réseau jouera un rôle essentiel dans le **partage des clefs de lecture**, dans la **création de réflexes**, et la **prévention des manipulations de l'information** à l'échelle locale.

ENGAGER LES COLLECTIVITÉS TERRITORIALES, LEURS ÉLUS ET LES COMMUNAUTÉS LOCALES

La pleine efficacité de la lutte contre les manipulations de l'information reposera sur la capacité à mobiliser le savoir et la capacité d'action des élus et des acteurs locaux. L'action menée à l'échelon national devra favoriser l'autonomie, la coopération et les initiatives locales. De nombreuses initiatives comme les rencontres organisées dans le cadre de NUMÉRIQUE EN COMMUN(S) témoignent en effet d'une capacité de mobilisation et d'action collective à l'échelle locale pouvant être soutenue à l'échelle nationale sans pour autant atteindre aux dynamiques locales.

PILIER

02

Réguler les plateformes en ligne et les services d'intelligence artificielle générative

Faire évoluer la gouvernance du numérique en responsabilisant les acteurs structurants de l'environnement informationnel – plateformes, moteurs de recherche, fournisseurs de services d'IA – face aux risques systémiques liés aux manipulations de l'information.

L'environnement informationnel contemporain est devenu un écosystème technique structuré par l'intermédiation numérique : moteurs de recherche, plateformes sociales, agents conversationnels, outils d'IA générative organisent aujourd'hui l'accès à l'information, la hiérarchie et la visibilité des contenus et la formation de l'opinion publique. Cette architecture algorithmique, sans équivalent dans les médias traditionnels régis par une responsabilité éditoriale claire, soulève des enjeux inédits en matière d'intégrité, de responsabilité, de pluralisme et de transparence.

L'arrivée des technologies d'IA générative, intégrées aux moteurs de recherche, aux réseaux sociaux ou aux systèmes d'exploitation et assistants numériques, renforce encore la complexité de cet environnement. Ces outils permettant la production et la diffusion de contenus synthétiques à grande échelle mais aussi de court-circuiter, tout en s'en nourrissant, les producteurs d'informations, qu'elles soient vérifiées ou non.

Face à la domination croissante de certaines plateformes et à la prolifération de comportements illicites ou préjudiciables, l'Union européenne a adopté des régulations ambitieuses, notamment le *Digital Services Act* (DSA), qui impose aux très grandes plateformes et très grands moteurs de recherche en ligne d'atténuer les risques systémiques qu'elles engendrent.

Ce règlement prévoit également un meilleur accès aux données pour les autorités de régulation, des garanties de transparence pour les utilisateurs, des options en faveur de flux non personnalisés, et un dispositif de signalement renforcé. En mars 2024, des lignes directrices ont été élaborées par la Commission européenne afin de préciser ce qui était attendu des plateformes dans l'application du DSA lors des périodes électorales.

Ultérieurement, une boîte à outils dédiée aux élections a été élaborée à destination des coordinateurs nationaux de services numériques afin de mettre en place toutes les modalités nécessaires permettant une meilleure mise en œuvre du DSA.

Dans ce contexte, la France entend assumer un rôle moteur pour une mise en œuvre exigeante et ferme du cadre européen, et pour travailler activement à l'amélioration de son efficacité opérationnelle.

Dans ce cadre, il est impératif d'utiliser pleinement les leviers juridiques à disposition pour pouvoir agir efficacement sur les plateformes numériques et les services d'IA générative, en particulier pendant les périodes électorales (OS5). Il s'agit de définir au niveau européen des règles techniques communes et précises permettant aux autorités nationales d'imposer, en période électorale, des mesures concrètes aux plateformes et aux services d'IA – adaptation des systèmes de recommandation, obligations renforcées de modération, exigences de transparence – afin de protéger le débat public. Un cadre clair rend ces interventions juridiquement solides, limite les risques de contestation et garantit leur conformité au droit européen.

Ensuite, la stratégie vise à établir un cadre de relations et de régulation rigoureux, sous peine de sanctions, entre les plateformes, les fournisseurs d'IA générative, les autorités, les chercheurs et la société civile (OS6). Ce cadre structuré sera le cœur d'une action collective favorisant le partage d'analyses, de signaux faibles et de pratiques de remédiation, dans une logique de coordination pérenne et de mutualisation des efforts.

La France poursuivra la consolidation de ses moyens d'analyse des risques informationnels liés à l'IA (OS7). En interaction constante avec les travaux de mise en œuvre du règlement européen sur l'IA et ceux poursuivis dans le cadre des analyses scientifiques portées au niveau national et international, le plateau opérationnel interdisciplinaire déjà constitué en France pour détecter, qualifier et anticiper les effets des IA génératives sur l'espace public sera renforcé.

Enfin, la stratégie nationale s'attaquera aux mécanismes de financement de la manipulation de l'information par la publicité programmatique (OS8). Pour cela, plusieurs priorités se dégagent : l'objectivation du phénomène, le soutien à l'établissement de référentiels dédiés, ainsi que le développement d'outils d'audits et de traçabilité.

OBJECTIF STRATÉGIQUE 5. S'ASSURER, DANS LE CADRE DU DROIT EUROPÉEN, DES MARGES DE MANŒUVRE NÉCESSAIRES SUR LES PLATEFORMES ET SERVICES D'IA GÉNÉRATIVE

L'importance prise par les plateformes et services d'IA générative dans la constitution de notre environnement informationnel exige de mobiliser tous les leviers possibles offerts par le cadre européen et national.

APPROFONDIR LA MISE EN ŒUVRE DU RÈGLEMENT EUROPÉEN SUR LES SERVICES NUMÉRIQUES

La régulation des services de la société de l'information repose encore, pour l'essentiel, sur les principes issus de la directive européenne 2000/31 dite « e-Commerce ». Celle-ci affirme notamment le **principe du pays d'origine**, selon lequel seul l'État membre d'établissement d'un service est compétent pour imposer des obligations spécifiques allant au-delà des normes européennes harmonisées, selon le degré d'harmonisation du champ concerné.

En outre, le règlement européen sur les services numériques (DSA) confie la supervision principale des très grandes plateformes et très grands moteurs de recherche à la Commission européenne, tout en confiant aux autorités du pays d'établissement des pouvoirs exclusifs à l'égard des autres acteurs visés par le règlement et en prévoyant des mécanismes de coordination avec et entre les États membres. Dans ce cadre, la capacité de la Commission et des États membres à agir pour protéger le débat public national, notamment en période électorale, peut et doit être renforcée.

Tandis que les États membres disposent d'une pleine compétence en matière de droit électoral, un point de tension a émergé dans l'appréciation de leur capacité d'intervention et d'édiction d'obligations formelles à la charge des plateformes en ligne. Un tournant jurisprudentiel a été amorcé par l'arrêt de la Cour de justice de l'Union européenne dans l'affaire *Google Ireland* (9 novembre 2023). Celui-ci reconnaît aux États autres que l'État d'établissement une capacité d'action ponctuelle et asymétrique, dès lors que : (i) les mesures envisagées visent un acteur précisément identifié ; (ii) les mesures envisagées sont nécessaires et proportionnées à l'un des objectifs légitimes définis à l'article 3, paragraphe 4, de la directive 2000/31, et (iii) l'État membre de destination du service a préalablement constaté une carence[4] de l'État membre d'établissement[5] après lui avoir demandé de prendre des mesures et lui avoir notifié, ainsi qu'à la Commission européenne, son intention de prendre lui-même de telles mesures. Un dialogue avec la Commission doit permettre de clarifier les marges d'action possibles de ce point de vue en matière électorale.

A cadre réglementaire constant, il s'agit également de poursuivre le travail engagé avec la Commission européenne pour préciser les mesures techniques spécifiques que devraient prendre les grandes plateformes en ligne avant, pendant et après une élection.

Les lignes directrices sur la protection des mineurs en ligne et les récentes évolutions en matière de contrôle de l'âge pour l'accès aux services de réseaux sociaux témoignent en effet de la possibilité de trouver des modes d'articulation entre les législations nationales et le cadre européen. De telles mesures pourraient demain porter sur **l'encadrement des systèmes algorithmiques des plateformes numériques lors des périodes électorales,** et pourraient être déployées lorsque la loi d'un État membre, en accord avec le droit de l'Union, prescrit des objectifs particuliers de communication en période électorale sur les médias en ligne. Elles pourront aussi porter, hors période électorale, sur la nécessaire transparence algorithmique, sur l'obligation de retrait de comptes inauthentiques, et sur la régulation de la publicité politique en ligne, dans le respect du règlement sur les services numériques.

Enfin, il importe d'ancrer dans une mise en œuvre rapide, ambitieuse et exigeante du DSA le

[4] On entend par carence l'absence d'action effective ou la défaillance manifeste de l'autorité compétente de l'État membre d'établissement dans l'exercice de ses pouvoirs de contrôle et d'exécution, notamment en cas d'inaction, de retard injustifié ou de mesures manifestement insuffisantes au regard des obligations applicables.

[5] Désigne l'État membre dans lequel le prestataire est établi pour la fourniture du service concerné, en principe le lieu de son siège ou de son établissement principal dans l'Union, et dont l'autorité est compétente à titre prioritaire au titre du principe du pays d'origine.

déploiement de mesures permettant :

- d'atteindre un haut niveau d'implication des autorités nationales dans la mise en œuvre du texte au niveau européen ;
- d'explorer les remèdes de niveau structurel touchant à l'architecture des plateformes et à leur interaction avec des acteurs tiers qui soient à même d'offrir des fonctionnalités alternatives de recommandation et de modération, avec application pleine et entière des obligations applicables à ces acteurs, notamment en matière de gestion des risques systémiques, et mise en place d'une évaluation des risques liés à ces nouvelles architectures ;
- de sécuriser les initiatives des autorités nationales en matière de protection du débat public pendant les périodes électorales ;
- de traiter spécifiquement les risques et les contenus issus des services d'intelligence artificielle générative.

ANALYSER ET TIRER LES CONSÉQUENCES DE LA RESPONSABILITÉ DES PLATEFORMES NUMÉRIQUES AU REGARD DE LEURS SYSTÈMES ALGORITHMIQUES

Par leurs fonctions de recommandation et de modération, pour les plateformes, et de génération de textes, pour les IA génératives, ces services peuvent revêtir une influence forte sur le contenu produit et ses modalités de réception par le public. Les plateformes maîtrisent la conception et les paramètres de leurs systèmes algorithmiques de recommandation, de personnalisation et de modération, ce qui doit pouvoir être analysé à l'aune des critères établis en jurisprudence afin d'en tirer toutes les conséquences nécessaires, tant en termes de responsabilité de ces acteurs vis-à-vis de leurs algorithmes que de capacité d'action des autorités nationales compétentes dans les États où leurs services sont présents.

Les réseaux sociaux dominants limitent l'émergence de formes de propagation, de modération ou d'accès au contenu qui soient alternatives à celles définies par l'entreprise. Outre une aisance d'usage et une satisfaction immédiate de l'utilisateur, ce verrou structurel peut aussi refléter des choix de conception ou de paramétrage conduisant à favoriser, voire amplifier, les risques de manipulation de l'information par le biais, notamment de l'exploitation de vulnérabilités algorithmiques cachées qu'il s'agit de pouvoir étudier, évaluer et dévoiler. La mobilisation de la communauté scientifique nationale et européenne à cette fin est aujourd'hui un impératif. Les autorités compétentes s'attacheront à documenter ces phénomènes dans le cadre des pouvoirs existants, notamment au moyen d'un projet de recherche dédié à l'analyse approfondie des méthodes algorithmiques mises en œuvre par certaines grandes plateformes en ligne.

Enfin, les remèdes structurels, tels que l'interopérabilité verticale[6] déjà permise par l'article 6(7) du règlement sur les marchés numériques (DMA) pour ce qui concerne les systèmes d'exploitation, méritent d'être explorés – dans le cadre des instruments européens et avec application pleine et entière des obligations applicables aux acteurs concernés et évaluation des risques propres à ces nouvelles architectures – **comme une voie offrant un rempart contre la captation des utilisateurs dans un modèle potentiellement favorable à la manipulation de notre environnement informationnel**. Des solutions alternatives d'interfaces, de recommandation ou encore de modération pourraient alors intervenir pour déjouer les structures ou comportements favorables à la manipulation de notre environnement informationnel.

[6] L'interopérabilité verticale désigne la possibilité pour des services ou outils tiers de se connecter techniquement à une plateforme ou à un système dominant afin de proposer, par-dessus son fonctionnement standard, des interfaces, des mécanismes de recommandation ou des dispositifs de modération alternatifs. Elle vise à réduire la dépendance aux seuls choix techniques et éditoriaux de l'acteur principal et à permettre l'émergence de fonctionnalités concurrentes ou complémentaires.

OBJECTIF STRATÉGIQUE 6. ORGANISER UN DIALOGUE STRUCTURÉ AVEC LES PLATEFORMES POUR LE PARTAGE D'INFORMATION AVEC LES AUTORITÉS PUBLIQUES ET LA SOCIÉTÉ CIVILE SPECIALISÉE

Structurer un cadre permanent de dialogue avec les plateformes et fournisseurs d'IA permettant le partage d'informations, d'analyses et de retours d'expérience avec les autorités publiques et la société civile spécialisée sur les phénomènes de manipulation de l'information.

Au-delà des évolutions juridiques engagées au niveau national et européen, la lutte contre les manipulations de l'information suppose un cadre structuré d'échange entre plateformes numériques, fournisseurs d'IA génératives, autorités publiques et acteurs spécialisés (recherche, vérification, OSINT, analyse des phénomènes informationnels). Les informations utiles à la compréhension des mécanismes de manipulation, des usages des plateformes et des effets des systèmes de recommandation demeurent aujourd'hui dispersées et inégalement accessibles. Cette situation limite la capacité d'analyse partagée et l'expression structurée des besoins des acteurs spécialisés.

L'expérience de l'Observatoire de la haine en ligne animé par l'ARCOM a démontré l'utilité d'un espace institutionnalisé d'échange associant plateformes, autorités et acteurs spécialisés, permettant le partage d'analyses, de pratiques et de retours d'expérience. Sur ce modèle, il sera institué un cadre permanent de dialogue structuré avec les plateformes et fournisseurs d'IA, dédié aux manipulations de l'information.

Plusieurs cadres sectoriels de co-régulation, au niveau européen comme national, fondés sur des espaces d'échange institutionnalisés entre régulateurs, acteurs privés et experts, ont démontré leur utilité pour améliorer la transparence des pratiques et la circulation d'informations pertinentes. À titre d'exemple, le Code de conduite de l'Union européenne sur la désinformation réunit plateformes, acteurs de la recherche et organisations spécialisées dans un cadre structuré d'échange et de transparence, avec des engagements de *reporting* et de partage d'information, et constitue aujourd'hui un dispositif de co-régulation articulé avec le règlement sur les services numériques.

Dans ce contexte, la mise en place d'un cadre national permanent de dialogue structuré avec les plateformes et fournisseurs d'IA vise à combler ce déficit d'échange organisé et à doter l'écosystème d'un espace stable de partage d'analyses et de connaissances sur les phénomènes de manipulation de l'information.

CONSTRUIRE UN DISPOSITIF STRUCTURÉ D'ÉCHANGE ENTRE PLATEFORMES, AUTORITÉS ET ACTEURS SPÉCIALISÉS

Ce cadre prendra la forme d'un dispositif d'échange régulier et formalisé, animé par une autorité identifiée, permettant la circulation d'informations, la confrontation d'analyses et la remontée structurée des observations et besoins de la société civile spécialisée vers les plateformes et les autorités.

Il aura pour fonctions, notamment : le partage d'informations, d'analyses, d'études de cas et de retours d'expérience ; la mise en commun d'observations et de typologies de manipulation ; la présentation par les plateformes et fournisseurs d'IA de leurs pratiques et évolutions ; la mise en place de mécanismes d'action rapides ; la remontée structurée de questions et recommandations des acteurs spécialisés.

La loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN) a déjà institué, pour les besoins de l'État, un réseau de coordination qui permet de développer le partage d'informations, la coopération et le dialogue entre les autorités compétentes, de travailler les problématiques d'articulation entre les différents cadres de régulation et de mener une réflexion stratégique commune sur les enjeux de la régulation du numérique.

Le dispositif proposé s'inscrit en articulation avec ce cadre de coordination interne à l'État et en constitue l'ouverture structurée vers les plateformes et la société civile spécialisée.

OBJECTIF STRATÉGIQUE 7. CONSOLIDER LA CAPACITÉ NATIONALE D'ÉVALUATION DES RISQUES POSÉS PAR L'INTELLIGENCE ARTIFICIELLE DANS LE CHAMP DE LA MANIPULATION DE L'INFORMATION

Créer une capacité d'expertise de référence, capable de qualifier, quantifier et anticiper les effets systémiques de l'IA sur la fiabilité de l'environnement informationnel.

L'essor de l'intelligence artificielle (IA), en particulier des technologies génératives et des systèmes agentiques, redéfinit profondément le paysage informationnel. Si ces outils offrent de nouvelles opportunités, ils introduisent également des risques systémiques majeurs, notamment en matière de production, d'amplification et de diffusion automatisée et coordonnée de contenus manifestement inexacts ou trompeurs.

Hypertrucages, génération de textes persuasifs, synthèse vocale, clonage d'identités, microciblage algorithmique : l'IA permet aujourd'hui de manipuler l'information à une échelle inédite, de manière difficilement détectable, et à un coût marginal. Ces usages soulèvent des menaces directes pour la sincérité du débat démocratique, notamment en période électorale ou en situation de crise.

Sur le plan réglementaire, le **règlement européen sur l'IA (*AI Act*)** introduit une typologie des risques fondée sur leur impact potentiel sur les droits fondamentaux et la sécurité. Certains systèmes utilisés à des fins de manipulation de l'information relèveront de la catégorie des **systèmes à haut risque**, voire des pratiques interdites (recours à des techniques manipulatrices, trompeuses ou subliminales). L'**obligation de transparence**, l'**étiquetage des contenus synthétiques**, et la **traçabilité des modèles** constituent les premiers garde-fous réglementaires.

Le **Rapport scientifique international sur la sécurité de l'IA avancée**[7] confirme par ailleurs le consensus croissant sur les risques que les modèles génératifs font peser sur l'environnement informationnel. En particulier, il existe un consensus scientifique sur le fait que les modèles génératifs (i) **facilitent les mécanismes de manipulation de l'information** ; (ii) **facilitent pour le moins une manipulation à grande échelle de l'opinion publique**, notamment en période électorale ou en situation de crise.

ÉVALUER ET RÉPONDRE AUX RISQUES LIÉS À L'IA : CRÉATION D'UN CENTRE D'EXCELLENCE IA X LMI AU SEIN DE VIGINUM

Face à ces constats, la France doit se doter d'une capacité d'évaluation robuste, pluridisciplinaire et coordonnée s'appuyant sur les activités de recherche et d'évaluation de son Institut national pour l'évaluation et la sécurité de l'intelligence artificielle (INESIA), les services d'expertise technique en IA au sein de l'État, comme le Pôle d'expertise de la régulation numérique (PEReN), l'Institut national de recherche en sciences et technologies du numérique (INRIA) et le Laboratoire national de métrologie et d'essais (LNE) ainsi que sur les expertises opérationnelles de VIGINUM et des administrations concernées.

Pour maximiser l'effet de la contribution de VIGINUM au travail collectif, son équipe DATALAB sera transformée en centre d'excellence IAxLMI. Le travail réalisé en source ouverte par ces acteurs permettra notamment de :

- fournir des outils et services clés en main aux **communautés de vérification de faits, aux médias, aux ONG et chercheurs** ;
- **renforcer l'appui à l'ARCOM**, au titre des missions découlant du règlement européen sur les services numériques (RSN, ou DSA en anglais), sur la modération et la vérification des algorithmes ;

[7] *Le International AI Safety Report 2026 est une évaluation internationale des capacités et des risques des systèmes d'intelligence artificielle avancée. Il a été lancé à la suite d'une résolution adoptée par 30 pays, ainsi que par des représentants de l'Union européenne et de l'ONU, lors du sommet sur la sécurité de l'IA de Bletchley Park. Inspiré du modèle du GIEC, il rassemble un panel d'experts internationaux afin de fournir une base scientifique commune aux décideurs publics.*

- **produire des évaluations indépendantes des risques** ; et appuyer les autorités publiques dans l'élaboration de réponses réglementaires ou techniques.

De manière complémentaire, la France doit apporter son soutien aux acteurs de l'écosystème mobilisés dans l'analyse et la détection des atteintes à l'intégrité de l'espace informationnel national. Ce soutien pourra prendre la forme d'appels à coopération ou financements ainsi que de différents modes de mise en visibilité.

OBJECTIF STRATÉGIQUE 8. TARIR LE FINANCEMENT DES INGÉRENCES NUMÉRIQUES ÉTRANGÈRES EN RENFORÇANT LA TRANSPARENCE DES SYSTÈMES DE PUBLICITÉ ET DE MONÉTISATION DES PLATEFORMES

Atténuer les risques systémiques liés au modèle économique des plateformes en ligne en matière d'ingérence numérique étrangère, et réduire la rentabilité des sites, comptes et chaînes impliqués dans des opérations de manipulation ou des pratiques frauduleuses, en renforçant la transparence des systèmes de monétisation et la traçabilité des flux publicitaires numériques.

Le modèle économique des grandes plateformes repose sur l'économie de l'attention, fondée sur trois piliers : une offre de services gratuits pour capter une audience massive et maximiser sa rétention, la transformation de cette audience en données comportementales, et la monétisation de ces données via des technologies publicitaires automatisées. En parallèle, des programmes de monétisation rémunèrent les créateurs et éditeurs de contenus « partenaires » selon le volume de vues et l'engagement de leurs publications.

Le rôle des mécanismes publicitaires et de monétisation dans le financement direct ou indirect de la manipulation de l'information est documenté de longue date, notamment dans les travaux académiques, les enquêtes journalistiques et le Code de conduite européen sur la désinformation. Les dispositifs existants ont toutefois montré leurs limites opérationnelles et leur caractère insuffisamment contraignant.

Les algorithmes de recommandation des réseaux sociaux amplifient les contenus générant le plus d'activité (clics, commentaires, partages, temps de lecture). Ces métriques, souvent liées à la charge émotionnelle des contenus, donnent un avantage indirect aux contenus polarisants voire polémiques. L'intérêt financier que représente la viralité de certaines thématiques peut ainsi motiver des acteurs opportunistes. l'institutionnalisation des programmes de redistribution crée ainsi une « économie » de la manipulation, pouvant favoriser des acteurs produisant massivement des contenus manifestement inexacts ou trompeurs.

Ce risque, identifié depuis plusieurs années, connaît une intensification avec l'essor des IA génératives, qui abaissent les coûts de production et de diffusion de contenus à grande échelle. Elles ne créent pas le phénomène, mais en modifient l'échelle et la vitesse, ce qui renforce l'enjeu de régulation des dispositifs de monétisation. La limitation de certains programmes à l'audience de quelques pays, dont la France, accroît le risque de ciblage opportuniste des utilisateurs français.

Au-delà des dispositifs de monétisation internes aux plateformes, la publicité programmatique constitue un canal majeur de financement de contenus à l'échelle du web. Fondée sur des enchères automatisées en temps réel pour l'achat d'espaces ciblés, et représentant près de 90 % des dépenses de publicité numérique, elle a industrialisé les flux publicitaires entre plateformes, intermédiaires et éditeurs tiers (sites, applications, environnements connectés). Cette automatisation, optimisée pour la performance et le coût, expose toutefois les annonceurs à un risque de placement involontaire sur des supports de faible valeur éditoriale ou diffusant de l'information, y compris lorsqu'ils sont opérés par des acteurs étrangers.

Le règlement européen sur les services numériques (DSA) fournit désormais un cadre juridique contraignant pour le traitement des risques systémiques liés aux plateformes, incluant la manipulation de l'information, les usages frauduleux des systèmes publicitaires et les dispositifs de monétisation. Les obligations de transparence (notamment articles 26 et 39) et les mécanismes d'évaluation et de mitigation des risques systémiques constituent le socle principal de l'action publique. La stratégie s'inscrit dans ce cadre et vise à en renforcer l'effectivité opérationnelle, dans une logique de contrôle, d'audit et, le cas échéant, de mesures correctrices et de sanctions.

Ces mesures s'articulent avec les obligations de gestion des risques systémiques du DSA et les procédures européennes d'enquête et de sanction, en s'appuyant sur des dispositifs techniques standardisés garantissant auditabilité, traçabilité publicitaire et identification publique des supports d'ingérence.

Atténuer les risques systémiques en matière d'ingérence numérique étrangère induits par les programmes de monétisation

La stratégie prévoit d'abord de définir à l'échelle nationale un référentiel cartographiant les dispositifs de monétisation des plateformes et de renforcer l'application des obligations de transparence pour les créateurs et éditeurs établis hors de France, qu'ils soient situés dans un autre État membre ou dans un pays tiers, diffusant des contenus politiques visant des audiences françaises, en complément des obligations déjà prévues par le règlement (UE) 2024/900 relatif à la transparence et au ciblage de la publicité à caractère politique, notamment lorsque les dispositifs de monétisation ou de promotion ne relèvent pas formellement de la publicité politique au sens de ce règlement (localisation de l'acteur, signataire du contrat, flux financiers, etc.). Ce référentiel servira de prototype et pourra être porté au niveau européen, dans le respect des compétences de l'Union européenne et du cadre harmonisé existant.

Plusieurs actions visent à responsabiliser les plateformes :

- exiger une transparence totale sur les relations commerciales avec des individus ou entités impliqués dans des opérations d'ingérence numérique étrangère documentées, notamment celles sous sanctions dans l'UE ;
- obliger les plateformes à mettre en place un guide de bonne conduite pour les contenus monétisables et prévoir des sanctions en cas de non-respect ;
- lutter contre les dérives des influenceurs et créateurs liées à l'ingérence numérique étrangère, en s'inspirant de la loi n°2023-451 du 9 juin 2023 sur l'encadrement de l'influence commerciale ;
- encourager la vérification de l'identité des administrateurs et de la fiabilité des contenus pour l'éligibilité aux programmes de monétisation ;
- exiger la suspension du financement de comptes diffusant de manière répétée ou coordonnée des informations trompeuses à des fins lucratives, avec transparence sur les comptes concernés.

Un référentiel technique dédié à la traçabilité des flux publicitaires

La stratégie prévoit également la définition d'un référentiel technique minimal pour assurer la traçabilité des flux publicitaires numériques. Une grille de conformité permettra d'évaluer la présence, la complétude et la cohérence de ces éléments. Cette traçabilité sera indispensable pour auditer les campagnes, détecter les parcours opaques ou frauduleux et limiter l'exposition des messages à des contextes non souhaités.

Elle permettra aussi de vérifier le respect des obligations de transparence des plateformes concernant les publicités politiques, notamment celles interdites ou contraires à leurs conditions d'utilisation avant des élections nationales.

Un registre public des supports manifestes d'opérations de manipulation

Un registre public recensera les sites ou chaînes identifiés comme supports manifestes d'ingérences numériques étrangères. Il reposera sur des évaluations indépendantes associant journalistes, chercheurs, experts OSINT, organisations indépendantes, et entités étatiques compétentes telles que VIGINUM. Les critères d'inclusion seront transparents : caractère manipulatoire des contenus, absence de transparence éditoriale, participation à des campagnes coordonnées.

Ce registre sera accessible librement, sous formats interopérables (fichiers téléchargeables, API), pour

intégration dans les outils des agences médias, plateformes publicitaires et acteurs publics. Il sera mis à jour régulièrement, horodaté, avec un dispositif contradictoire permettant aux éditeurs de contester leur inclusion. Ce registre ne remplacera pas l'appréciation de la légalité des contenus mais constituera un outil de transparence et de responsabilisation dans une logique de co-régulation.

PILIER

03

Renforcer la capacité opérationnelle de lutte contre les ingérences numériques étrangères

Structurer une réponse opérationnelle souveraine, réactive et crédible face aux manipulations de l'information, en consolidant les capacités opérationnelles détection, de caractérisation, d'imputation et de réponse et en renforçant l'écosystème technologique national.

Assurer l'intégrité du débat public à l'ère numérique suppose de disposer de capacités nationales pleinement opérationnelles, capables de détecter les manœuvres hostiles, d'en comprendre les ressorts, et d'y répondre avec réactivité et discernement. Ce socle opérationnel, encore en consolidation, constitue l'armature stratégique de la lutte contre les ingérences numériques étrangères. Face à la montée en puissance de cette menace informationnelle, la France s'engage à construire une réponse cohérente, graduée et crédible, articulant les dimensions techniques, juridiques, diplomatiques et industrielles.

La première condition d'efficacité est la détection précoce partagée. C'est l'objectif poursuivi par le renforcement des capacités de veille, de détection et de caractérisation des ingérences numériques étrangères (OS9). Les campagnes visées, de plus en plus furtives et hybrides, exigent une capacité de vigilance continue et partagée. Le dispositif COLMI, transformé en une plateforme de coordination opérationnelle et technique, jouera un rôle central dans cette communauté. Le réseau diplomatique, notamment à travers ses postes à l'étranger, apportera un appui décisif à cette stratégie, en assurant une veille contextuelle renforcée dans les zones les plus vulnérables. La montée en puissance du dispositif de veille du ministère de l'Europe et des affaires étrangères (MEAE) permettra en parallèle de mieux détecter les campagnes d'influence et de communication stratégique d'acteurs étrangers.

Mais détecter ne suffit pas : encore faut-il pouvoir répondre. La structuration d'une doctrine interministérielle de réponse aux opérations d'ingérences numériques étrangères et plus largement des manipulations de l'information d'origine étrangère (OS10) constitue le deuxième pilier de la stratégie. Placé sous l'autorité du SGDSN et du MEAE, le dispositif interministériel proposera, en fonction de chaque situation, des stratégies combinant différents leviers – techniques, diplomatiques, judiciaires, économiques ou communicationnels. Leur mobilisation concertée, y compris dans un cadre multilatéral, européen ou allié, permettra de restaurer la confiance publique, d'imposer un coût à l'agresseur et de prévenir la récidive.

Cette réponse suppose une coordination fluide entre les administrations concernées, dans le respect du droit et des orientations politiques validées, et ne portant pas préjudice aux compétences propres de chaque administration, qui demeure capable d'agir selon ses prérogatives et son cadre juridique propre.

Cette réponse interministérielle s'appuie aussi sur une capacité judiciaire renforcée (OS11). Pour garantir son efficacité, un plan d'action judiciaire sera déployé : renforcement du parquet compétent, montée en compétence des juridictions territoriales et amélioration de la coordination entre services administratifs et judiciaires. Un accent particulier sera mis sur la protection du processus électoral.

Enfin, pour consolider dans la durée les capacités d'analyse, la France soutient l'émergence d'une filière souveraine d'investigation en sources ouvertes (OS12). L'OSINT constitue aujourd'hui un levier essentiel, encore largement structuré par des communautés intéressées, militantes, journalistiques ou académiques agissant hors cadre institutionnel. L'État favorisera l'essor d'un écosystème technologique de confiance, adossé à des outils souverains, des environnements sécurisés et des passerelles public-privé.

La stratégie nationale valorisera aussi les compétences issues de la communauté OSINT indépendante, par des mécanismes concrets : microfinancements, intégration dans les activités de l'Académie et des réseaux de coopération constitués. Cette articulation entre expertise citoyenne et mission d'intérêt général viendra enrichir les capacités de veille et renforcer la résilience collective.

OBJECTIF STRATÉGIQUE 9. RENFORCER LES CAPACITÉS DE DÉTECTION ET CARACTÉRISATION DES INGÉRENCES NUMÉRIQUES ÉTRANGÈRES

Consolider la capacité nationale de veille, de détection et de caractérisation d'une ingérence numérique étrangère, de façon continue, mutualisée et distribuée, pour détecter précocement les campagnes hostiles et en qualifier rigoureusement la portée, les mécanismes et les auteurs.

Face à la complexité croissante des campagnes de manipulation de l'information, la première exigence est celle de la détection précoce. Les ingérences numériques étrangères peuvent prendre des formes multiples et s'appuyer sur une variété de vecteurs : réseaux sociaux, plateformes de vidéo, messageries chiffrées, forums spécialisés, etc.

Le tempo opérationnel de la LMI en fait un exercice de gestion de crise permanent exigeant des échanges techniques quasiment continus pour traiter la menace. Pour qu'une stratégie de réponse soit efficace, encore faut-il disposer d'un système d'alerte et de réponse fiable et réactif, fondé sur une capacité de veille, de détection et de caractérisation collectif, performant et souverain.

RENFORCER LE DISPOSITIF NATIONAL DE VEILLE, DE DÉTECTION ET DE CARACTÉRISATION D'UNE INGÉRENCE NUMÉRIQUE ÉTRANGÈRE

Au niveau national, le cœur opérationnel de la caractérisation des ingérences numériques étrangères est incarné par le COLMI, instance de coordination opérationnelle animée par VIGINUM. Pour répondre au rythme imposé par les adversaires, cette structure évoluera vers une configuration plus permanente, réunissant de manière périodique l'ensemble des parties prenantes techniques et stratégiques concernées.

En parallèle, une capacité d'anticipation stratégique devra être renforcée pour prévenir l'émergence de campagnes. Elle reposera sur une diversité de méthodes croisées : exploitation en sources ouvertes (OSINT), traitement algorithmique de données massives, modélisation des dynamiques de propagation, et analyse experte. Des partenariats structurés avec le monde académique, les plateformes, les laboratoires publics et privés viendront enrichir cette capacité d'analyse distribuée.

La montée en puissance des capacités de veille de contenus du MEAE appuyée sur le réseau diplomatique apportera une capacité importante en la matière.

Enfin, seront déployés les dispositifs interministériels (instances, canaux d'échanges, désignation de points focaux) nécessaires à la circulation des informations avec les administrations et institutions ayant un rôle à jouer dans la détection mais aussi dans la diffusion de l'information sur les modalités de manipulation d'informations à l'œuvre.

APPUYER LA DÉTECTION DEPUIS L'ÉTRANGER : LE RÔLE DU RÉSEAU DIPLOMATIQUE

La **capacité de veille, de détection et de caractérisation internationale** constitue un levier de complément utile, en particulier dans les zones sensibles ou peu couvertes techniquement. Le réseau diplomatique français, piloté par le ministère de l'Europe et des affaires étrangères à Paris, pourra contribuer à la **remontée d'éléments de contexte**, à l'**identification d'acteurs hostiles** et à l'**alerte en cas de séquences sensibles** (périodes électorales, tensions politiques, attaques informationnelles ciblées).

Dans cet objectif, plusieurs actions seront encouragées :

- cartographier les écosystèmes informationnels à l'échelle locale et régionale (plateformes dominantes, relais narratifs, figures hostiles) ;
- entretenir une veille régulière sur les contenus et les canaux stratégiques, au-delà des seuls acteurs institutionnels ;

- renforcer la coordination interministérielle pour faciliter les échanges de signaux faibles, l'alignement des autorités dans leur expression extérieure et le partage d'outils.

OBJECTIF STRATÉGIQUE 10. STRUCTURER ET COORDONNER LA RÉPONSE DE L'ÉTAT AUX INGÉRENCES NUMÉRIQUES ÉTRANGÈRES

Définir une doctrine opérationnelle de réponse aux ingérences numériques étrangères, fondée sur une mobilisation graduée et coordonnée de l'ensemble des leviers de l'État, et adaptée aux exigences particulières de la période électorale.

La lutte contre les manipulations de l'information ne se limite pas à la détection des campagnes hostiles. Elle suppose la capacité à y répondre de manière résolue, dans le respect du droit, avec des effets dissuasifs ou correctifs clairement identifiés.

À cette fin, la France s'appuie sur une instance de coordination interministérielle spécifique, placée sous l'autorité du SGDSN et du MEAE. Il s'agit non seulement de gérer les conséquences d'un événement, mais surtout d'agir sur les causes, en élaborant des **stratégies de réponse interministérielles** face aux campagnes identifiées d'ingérence numérique étrangère et plus largement des manipulations étrangères de l'information.

Chaque réponse interministérielle est construite en fonction de la nature et de la gravité de l'ingérence, de son origine présumée, de l'efficacité et de la disponibilité des leviers mobilisables, ainsi que du cadre de coopération nationale ou internationale pertinent.

MOBILISER L'ENSEMBLE DES LEVIERS DE RÉPONSE DE L'ÉTAT

Ce dispositif s'appuie sur une boîte à outils complète face aux ingérences numériques étrangères, combinant plusieurs types de leviers d'action pouvant être combinés, activés de manière graduée ou simultanée, selon différentes temporalités. Ces leviers peuvent être :

- **communicationnels :** actions de rétablissement des faits, mobilisation des relais d'opinion et des partenaires de confiance, publication régulière de bulletin d'information sur les ingérences numériques étrangères ;
- **diplomatiques :** condamnations publiques, actions de rétorsion, canaux de désescalade, mesures de confiance ;
- **judiciaires :** ouverture de procédures contre les auteurs ou leurs relais ;
- **économiques :** activation de régimes de sanctions nationaux ou européens ;
- **militaires :** mobilisation en appui de l'action des autres administrations ou mise en œuvre des leviers d'actions militaires selon le cadre et la chaîne de commandement des opérations ;
- **techniques :** entrave de capacités techniques adverses, diffusion ciblée d'éléments d'analyse ou d'alerte.

Le **choix de l'attribution d'une opération d'ingérence à un commanditaire** – publique, confidentielle, bilatérale ou coordonnée – est un outil stratégique à part entière. Il est décidé en fonction des effets recherchés : découragement, signalement diplomatique, clarification publique, ou construction d'un consensus international.

C'est dans ce cadre par exemple que s'inscrivent les formes nouvelles de **ripostes immédiates sur les réseaux sociaux tel que le compte FRENCH RESPONSE mis en place et piloté par le MEAE**. En amont, cette dynamique mérite d'être soutenue par la diffusion d'une culture et de savoir-faire communicationnels mettant en capacitant une variété d'acteurs d'assurer une communication pro-active sur les canaux et selon les modalités les plus appropriées. Ce qui concerne le réseau diplomatique mais, plus largement, au sein des autres ministères et, au-delà, des acteurs non-étatiques.

Par cette **doctrine de réponse structurée**, la France entend **imposer un coût croissant aux agresseurs**, réduire l'incitation à la récidive et démontrer sa capacité à protéger, de manière crédible et

proportionnée, **l'intégrité de sa vie démocratique face aux campagnes hostiles**.

Se doter d'un dispositif spécifique pour apprécier et coordonner la réponse en période électorale

En période électorale, la capacité désormais acquise par l'État à détecter et caractériser des opérations d'ingérence numérique étrangère fait naître un enjeu spécifique de décision publique : intervenir pour dénoncer ou contrer une manœuvre peut influencer le débat démocratique, tandis que l'inaction peut laisser prospérer une manipulation de l'information susceptible d'altérer manifestement la sincérité du scrutin.

Dans ce contexte, cette doctrine de réponse s'appuie sur un nouveau dispositif dédié : le **Réseau de coordination et de protection des élections (RCPE)**, placé sous la coordination du Secrétariat général de la défense et de la sécurité nationale.

Le RCPE réunit les administrations et autorités indépendantes compétentes en matière électorale : l'ARCOM, la CNCCFP, le secrétariat général du Gouvernement, le ministère de l'Intérieur, VIGINUM et le Comité éthique et scientifique, chargé de suivre son activité. Il est chargé d'évaluer la menace d'ingérences numériques étrangères pendant la période des élections municipales, de proposer le cas échéant la mise en œuvre de mesures de réponse, d'informer le grand public de manière régulière et périodique.

Ce réseau, composé exclusivement d'acteurs administratifs et d'autorités indépendantes, est dépourvu de toute fonction politique ou partisane. Il a pour finalité d'objectiver l'analyse de la menace et d'éclairer la puissance publique sur la nature, le moment et les modalités de son intervention en période électorale, dans un contexte où toute action – comme toute absence d'action – est susceptible d'avoir un impact sur le débat démocratique.

Ce dispositif permet ainsi d'articuler, en temps réel et de manière proportionnée, les leviers administratifs, judiciaires, techniques, communicationnels et diplomatiques mobilisables, tout en respectant les compétences propres de chaque acteur. Il contribue à garantir une réponse cohérente, graduée et lisible de l'État face aux tentatives d'ingérence numérique étrangère visant le processus électoral, tout en préservant la neutralité de l'action publique et la sincérité du scrutin.

Sa pérennisation et son extension sera étudiée de façon à garantir de façon durable la protection de l'ensemble des élections contre toute forme d'ingérence.

OBJECTIF STRATÉGIQUE 11. RENFORCER L'ACTION JUDICIAIRE EN MATIÉRE DE LUTTE CONTRE LA MANIPULATION DE L'INFORMATION, NOTAMMENT EN PÉRIODE ÉLECTORALE

Doter l'autorité judiciaire des moyens opérationnels de lutter contre les manipulations de l'information, afin d'identifier, de poursuivre et de sanctionner efficacement les acteurs de campagnes d'ingérence numérique étrangère, notamment en période électorale.

La lutte contre les ingérences numériques étrangères, et plus largement les opérations de manipulation de l'information, suppose un continuum cohérent entre les actions administratives, diplomatiques, techniques et judiciaires. Dans ce cadre, l'action judiciaire constitue un levier essentiel d'entrave et de sanction, permettant de viser directement les acteurs humains ou techniques de campagnes hostiles.

À ce jour, de nombreuses qualifications pénales et dispositifs du code civil existent (provocation à la haine, atteinte aux intérêts fondamentaux de la Nation, diffamation ou injures, altération manifeste de la sincérité du scrutin).

L'enjeu réside d'abord dans l'opérationnalisation du cadre applicable afin qu'il puisse, dans les faits, offrir des mesures de répression visant les personnes physiques ou morales qui participent délibérément à la diffusion automatisée, massive ou coordonnée, de contenus manifestement inexacts ou trompeurs, dans l'intérêt d'une puissance étrangère ou sous son influence, et dans le but de porter atteinte aux intérêts fondamentaux de la Nation.

Nonobstant la mise en œuvre rapide, dans un cadre administratif, de mesures de retrait, de blocage ou de déréférencement, ce cadre judiciaire doit permettre l'ouverture d'enquêtes dédiées pouvant conduire à la délivrance de réquisitions judiciaires aux plateformes numériques et au suivi de la qualité et de la quantité des retours effectués, à l'engagement de poursuites à l'encontre des auteurs ou relais identifiés et à la caractérisation judiciaire d'une campagne d'ingérence, à l'aide de preuves recueillies dans le respect du principe du contradictoire.

Les élections sont des cibles privilégiées des ingérences numériques étrangères. Pour préserver la sincérité du débat public dans un des moments les plus sensibles de la vie publique, la France structurera un dispositif opérationnel de réponse en période électorale. Dans cette boite à outils, les **circonstances aggravantes** prévues pour les ingérences étrangères pourront être mobilisées.

RENFORCER LA RÉPONSE JUDICIAIRE DANS TOUTES SES DIMENSIONS

Afin de rendre l'action judiciaire plus rapide et plus opérationnelle, notamment en période électorale, la stratégie s'appuiera sur une **boîte à outils juridique structurée autour d'évolutions ciblées du droit applicable et de leur mise en œuvre effective**.

- **En amont des scrutins : renforcer et étendre le référé électoral** (art. L. 163-2 du code électoral) La France poursuivra l'opérationnalisation du référé dit « anti-fake news » et engagera les adaptations nécessaires pour **en élargir le champ d'application** aux **scrutins locaux, notamment municipaux**. L'objectif est de disposer d'un levier d'intervention rapide (48 heures) pendant les campagnes électorales, lorsque des contenus sont diffusés en ligne de manière délibérée, artificielle ou automatisée et massive.

- **Après le scrutin : renforcer la répression des atteintes à la sincérité du scrutin et mieux prendre en compte l'extranéité de la menace** (art. L. 97 du code électoral et art. 411-12 du code pénal). La France portera les évolutions nécessaires afin que la diffusion de fausses nouvelles ou de manœuvres frauduleuses altérant la sincérité d'un scrutin puisse être sanctionnée de manière plus forte, par une réévaluation du quantum de peine prévu à l'article L. 97 du code électoral. Elle portera également l'adaptation permettant d'étendre l'application de la circonstance aggravante d'ingérence étrangère à cette infraction, afin de renforcer la réponse pénale lorsque les faits servent les intérêts d'une puissance étrangère ou s'inscrivent sous son influence.

En complément, pour garantir l'efficacité de l'action judiciaire, un plan d'action global sera déployé autour de deux axes :

- **la mobilisation des parquets compétents** : le parquet de Paris dispose de sections spécialisées dotées de moyens dédiés pour traiter les dossiers les plus complexes, en articulation étroite avec les services spécialisés de l'État. Cette mobilisation s'appuie d'ores et déjà sur un cadre d'instructions rénové, visant d'une part à améliorer l'identification des faits et des qualifications pénales mobilisables et d'autre part à renforcer la coordination des parquets territoriaux avec le parquet de Paris, auquel a été dévolu une compétence exclusive permettant la centralisation du traitement de certaines infractions afin d'assurer une réponse pénale cohérente, spécialisée et dissuasive[8].
- **la consolidation de la coopération judiciaire internationale** : la France renforcera son engagement dans les mécanismes européens et bilatéraux, pour garantir une coordination efficace des enquêtes transnationales et faciliter les procédures d'extradition.

[8] Circulaire du garde des Sceaux du 26 janvier 2026 relative à la mobilisation de l'autorité judiciaire dans la lutte contre les manipulations de l'information, accompagnée d'un « focus » à destination des magistrats relatif à l'appréhension judiciaire de la lutte contre les manipulations de l'information ; circulaire du garde des Sceaux du 21 janvier 2026 relative à la mobilisation de l'autorité judiciaire dans la lutte contre les ingérences étrangères.

OBJECTIF STRATÉGIQUE 12. SOUTENIR L'ÉVOLUTION DE L'ÉCOSYSTÈME NATIONAL CAPACITAIRE EN MATIÈRE D'INVESTIGATION NUMÉRIQUE EN SOURCE OUVERTES

Structurer une filière française d'outils, de services et de compétences dédiés à l'OSINT, au service des missions de détection, d'analyse et de lutte contre les manipulations de l'information en ligne.

La recherche en sources ouvertes (OSINT) est devenue un pilier incontournable de l'action publique en matière de lutte contre les manipulations de l'information. Ce domaine d'expertise transversal repose sur la capacité à collecter, traiter et analyser de grandes quantités de données issues de sources ouvertes, afin d'y détecter, des signaux faibles révélateurs de manipulations. Dans un contexte de sophistication croissante des ingérences numériques étrangères, l'exploitation méthodique des données librement accessibles constitue une capacité stratégique. Elle permet de repérer les campagnes malveillantes, d'en comprendre les dynamiques, et d'anticiper leur diffusion.

Pour en tirer parti, **il est indispensable de disposer de capacités de collecte efficaces, diversifiées et résilientes**, notamment sur le web et les réseaux sociaux. La diversité des plateformes, la variabilité de leurs architectures et la nécessité d'opérer à des rythmes proches du temps réel imposent une grande agilité technique.

Au surplus, ces environnements évoluent en permanence : pour des raisons fonctionnelles ou de sécurité, les plateformes modifient fréquemment leurs interfaces et restreignent la collecte automatisée. Dans ce contexte, **il ne suffit plus de disposer d'un outil unique ou d'une technologie isolée**. Il faut disposer d'un ensemble distribué et adaptable de solutions, évitant toute dépendance excessive à un prestataire, une méthode ou un format technique.

La France dispose de capacités OSINT opérationnelles, notamment dans des environnements spécialisés, qu'ils soient institutionnels, académiques ou privés. Plusieurs acteurs nationaux développent des outils et services prometteurs, illustrant le potentiel et la vitalité de l'écosystème national.

Toutefois, ces initiatives restent trop dispersées et insuffisamment coordonnées à l'échelle nationale. Leur potentiel reste limité par un faible niveau de mutualisation et l'absence d'un cadre structurant, favorable à l'industrialisation, à la souveraineté technologique et à l'interopérabilité. Structurer cet écosystème constitue désormais un enjeu stratégique majeur.

STRUCTURER UNE FILIÈRE SOUVERAINE, INNOVANTE ET RÉSILIENTE DE L'OSINT

Le tissu industriel français compte d'ores et déjà plusieurs entreprises proposant des solutions OSINT de qualité, innovantes et compétitives. Ce vivier d'acteurs, encore en phase de consolidation, mérite d'être pleinement soutenu pour atteindre un niveau de maturité industrielle et répondre aux besoins croissants des institutions et de la société civile.

L'intervention de la puissance publique dans ce domaine repose sur au moins trois facteurs majeurs :

- **économique** : soutenir des entreprises françaises créatrices d'emplois et de valeur sur le territoire dans le domaine de la détection et de la caractérisation ;
- **technologique** : garantir la résilience et l'indépendance des capacités face à un environnement numérique en évolution rapide ;
- **sécuritaire** : assurer la maîtrise des chaînes techniques, la protection des données, et le respect du cadre légal applicable.

La France affirme son ambition de structurer et renforcer une filière nationale de l'OSINT, souveraine, innovante et interopérable, capable de répondre aux besoins croissants des institutions publiques, des chercheurs, des journalistes et de la société civile.

Cette filière reposera sur une politique industrielle partagée selon trois principes :

- **des outils technologiques mutualisables**, conçus par des acteurs français ou européens, dans le respect des cadres juridiques en vigueur ;
- **des environnements sécurisés** pour le traitement des données ouvertes, adaptés aux usages des analystes ;
- **des passerelles opérationnelles** entre la commande publique, les laboratoires de recherche et les startups du secteur, pour soutenir l'innovation.

Un dialogue structuré entre l'État et l'écosystème permettra d'identifier les priorités, d'orienter les investissements stratégiques, et de favoriser la mutualisation des approches entre acteurs institutionnels et civils. Les dispositifs existants (France 2030, Bpifrance, commande publique) seront mobilisés pour accompagner durablement les entreprises du domaine.

PRENDRE EN COMPTE ET ACCOMPAGNER LES COMPÉTENCES OSINT ISSUES DE LA SOCIÉTÉ CIVILE

Il existe en France une communauté d'analystes OSINT issue de parcours variés – recherche, journalisme, développement, anciens milieux institutionnels – qui contribue, de manière indépendante, à l'analyse de phénomènes informationnels en sources ouvertes. Ces compétences constituent un apport utile à la compréhension de l'environnement informationnel numérique.

Sans remettre en cause leur indépendance ni leur diversité d'organisation, la stratégie nationale vise à mieux identifier ces expertises et à faciliter, lorsque cela est pertinent, leurs interactions avec les acteurs publics et académiques.

À cette fin, pourront être étudiés différents leviers d'appui proportionnés et non contraignants, tels que des dispositifs légers de soutien à des travaux ou projets ciblés dans le cadre du plan France 2030.

PILIER

04

Assurer, avec nos alliés, l'existence d'un espace informationnel libre, ouvert et sécurisé

Construire une stratégie internationale cohérente et ambitieuse, fondée sur des coopérations concrètes, un appui au renforcement des capacités démocratiques et une présence active dans les enceintes normatives, pour garantir la résilience globale face aux manipulations de l'information.

À l'heure où certaines puissances cherchent à faire de l'espace numérique un champ de confrontation idéologique et stratégique, la France réaffirme son attachement à un espace informationnel libre, ouvert, pluraliste et sécurisé. Dans cette optique, la France entend jouer un rôle moteur pour promouvoir le droit, la transparence et la souveraineté des sociétés ouvertes et démocratiques. Elle s'appuiera pour cela sur ses alliances, ses partenariats et son savoir-faire reconnu, pour structurer une diplomatie de la résilience informationnelle autour de quatre chantiers complémentaires.

Structurer une réponse européenne à la menace informationnelle : construire une approche fédérative des services de détection au sein de l'Union européenne (OS13) afin de disposer d'un réseau fonctionnel. La France dispose d'un modèle opérationnel reconnu, adossé à un cadre juridique robuste. Dans le cadre du bouclier démocratique européen porté par l'Union européenne, la France est en faveur de l'émergence d'une communauté européenne de la LMI, notamment à travers la diffusion de bonnes pratiques opérationnelles de détection, l'accompagnement des États membres qui souhaitent renforcer leurs capacités opérationnelles, le développement de l'interopérabilité au sein de l'Union européenne en matière de lutte contre les manipulations de l'information ou encore le renforcement de la coopération avec les États tiers (États candidats, affinitaires dans le voisinage).

Cibler les efforts de renforcement capacitaire sur les États et zones les plus vulnérables : définir une stratégie de développement capacitaire fondée notamment sur un agenda des échéances démocratiques (OS14). Dans les régions où la démocratie est fragile, les campagnes de manipulation peuvent avoir un effet déstabilisateur majeur. La France s'engage donc à contribuer à définir une stratégie de renforcement des capacités opérationnelles, notamment calée sur un agenda d'échéances démocratiques critiques (élections, référendums, etc.). Cette action s'appuiera notamment sur les instruments de l'Union européenne existants ainsi que sur des partenariats bilatéraux.

Coordonner la réponse démocratique dans les enceintes multilatérales : mobiliser pleinement les cercles européens, transatlantiques et onusiens (OS15). Au sein de l'Union européenne, la France poursuivra son engagement actif auprès du Service européen pour l'action extérieure, de la Commission et du Parlement européen, pour faire avancer une doctrine commune de LMI.

Tout en étant consciente des difficultés et divisions des enceintes multilatérales internationales, la France continuera d'y marquer un engagement fort. Au sein du G7, elle promouvra une meilleure coordination des dispositifs nationaux, en lien avec les engagements pris dans le cadre du Code de conduite pour l'intégrité de l'information. À l'OTAN, elle soutiendra l'intégration des manipulations informationnelles au sein la doctrine de l'Alliance. À l'ONU, elle défendra une approche fondée sur la transparence, la proportionnalité et la souveraineté informationnelle, notamment dans le cadre du Global Digital Compact et dans les travaux conduits au sein de l'UNESCO. Il en ira de même au sein de l'OCDE, et la France continuera d'être active dans le monde francophone au travers de l'organisation internationale de la francophonie.

Enfin, la France devra **investir les enceintes** permettant d'accueillir un dialogue multilatéral associant acteurs privés et publics sans pour autant dépendre des choix stratégiques défavorables au multilatéralisme pouvant être opérés par certains États ou acteurs privés. En parallèle, elle investira les **enceintes normatives et les coalitions capacitaires** car une part croissante de la régulation de l'espace informationnel se joue dans des enceintes de standardisation technique.

OBJECTIF STRATÉGIQUE 13. CONSTRUIRE UNE APPROCHE COORDONNÉE ENTRE SERVICES DE DÉTECTION ET D'ANALYSE DES CAMPAGNES DE MANIPULATION AU SEIN DE L'UNION EUROPÉENNE

Structurer une communauté opérationnelle au sein de l'Union européenne, articulée autour d'agences nationales spécialisées, afin de renforcer la détection coordonnée et la réponse collective aux menaces informationnelles.

Dans un contexte de tensions géopolitiques accrues et de déstabilisation numérique croissante, l'Union européenne s'est engagée à bâtir un bouclier démocratique européen. Ce projet vise à protéger la stabilité institutionnelle, l'intégrité des processus électoraux et la confiance dans le débat public. Il repose sur une conviction centrale : chaque État membre doit pouvoir détecter et contenir, avec réactivité, les tentatives d'ingérences numériques étrangères visant ses citoyens, ses institutions ou ses partenaires.

Dans ce cadre, la France bénéficie d'une légitimité particulière. Son dispositif de lutte contre les manipulations de l'information dans l'espace numérique constitue une référence européenne. Ce modèle permet à la France de jouer un rôle moteur dans la construction d'une capacité partagée entre États membres, fondée sur la subsidiarité, la coopération opérationnelle et la montée en compétence collective.

FAIRE NAÎTRE UNE EXCELLENCE EUROPÉENNE EN MATIÈRE DE LMI

L'objectif est de faire émerger une **excellence européenne en matière de lutte contre les manipulations de l'information dans l'environnement numérique**, en structurant une véritable communauté de la LMI entre les institutions européennes et les États membres, autour de trois axes majeurs :

- **partage des bonnes pratiques et méthodologies opérationnelles** au sein de l'UE, en s'appuyant notamment sur l'approche française, fondée sur l'analyse des comportements inauthentiques et la recherche en sources ouvertes.
- **accompagnement des États membres souhaitant renforcer leurs capacités** et favoriser la mise en place d'agences ou de services gouvernementaux opérationnels dédiés à la LMI et à la détection des ingérences numériques étrangères.
- **renforcement de la mise en réseau et de l'interopérabilité** entre les États membres, les institutions européennes et la société civile, afin d'améliorer la coopération et de favoriser le partage des connaissances sur la menace informationnelle.

Ces priorités visent à consolider une communauté d'acteurs de la lutte contre les manipulations de l'information (États membres, institutions de l'UE, société civile) en mesure de détecter, qualifier et documenter les menaces informationnelles avec une granularité territoriale et une vision partagée. Il constituera l'un des fondements du bouclier démocratique européen, visant à ériger une capacité collective de réponse aux manipulations de l'information émanant d'acteurs étrangers, dans le respect des prérogatives souveraines des États membres dans la protection de leurs débats nationaux

OBJECTIF STRATÉGIQUE 14. DÉFINIR UNE STRATÉGIE INTERNATIONALE DE RENFORCEMENT DES CAPACITÉS D'ACTION DE NOS PARTENAIRES

Structurer un appui international ciblé et solidaire en matière de LMI, fondé sur les échéances démocratiques sensibles, les contextes géopolitiques critiques et la demande locale de renforcement de capacité, en lien étroit avec les dispositifs européens existants.

À mesure que les campagnes d'ingérences numériques étrangères se sophistiquent, elles visent de plus en plus directement les processus démocratiques : élections nationales, référendums, consultations citoyennes, débats législatifs ou sociaux majeurs. Ces séquences sensibles deviennent des cibles privilégiées pour des puissances étrangères hostiles, qui y voient des opportunités de polarisation, de déstabilisation, de renforcement de la confusion voire du chaos et *in fine* de perte de confiance dans les institutions.

Pour répondre à cette menace, la France opère déjà et développera encore un soutien développera un soutien aux partenaires étrangers susceptibles d'agir contre les manipulations de l'information pour renforcer les capacités nationales en amont et en fonction des temps démocratiques critiques, là où les États en expriment la demande.

UN APPUI SOLIDAIRE, AGILE, ET ANCRÉ DANS LES PARTENARIATS EUROPÉENS

Cette stratégie s'appuiera sur plusieurs leviers :

- **l'élaboration d'un agenda partagé des échéances démocratiques à haut risque**, piloté par le MEAE, le Service européen pour l'action extérieure (SEAE), l'Union européenne et d'autres partenaires internationaux, pour cartographier les zones de vulnérabilité et anticiper les besoins de nos alliés.
- **la création de missions d'appui technique**, mobilisant des expertises françaises et européennes, pouvant être déployées rapidement à l'invitation d'un État, avant ou pendant une échéance électorale.
- **la consolidation d'un pilier européen de renforcement capacitaire** (*capacity building*) en matière de lutte contre la manipulation de l'information, notamment dans le prolongement du bouclier démocratique européen. Ce pilier permettra d'assurer une coordination des efforts entre États membres et institutions européennes.

FAIRE DE L'EUROPE UN EXPORTATEUR DE STABILITÉ INFORMATIONNELLE

En intégrant cette action dans le cadre européen, la France entend faire de l'Union un pôle de projection de stabilité démocratique. Cela suppose d'ancrer le ***capacity building*** **en LMI dans les instruments de politique extérieure de l'Union européenne**, à l'image de ce qui existe pour la cybersécurité ou la protection des processus électoraux. La stratégie française promouvra :

- **l'intégration systématique de la LMI dans les programmes d'assistance électorale ou de renforcement de l'État de droit** financés par l'Union européenne ;
- **la création de modules LMI dans les programmes européens d'assistance technique** là où cela demeure nécessaire ;
- **la poursuite du développement d'un vivier d'experts LMI européens** mobilisables rapidement à l'international, dans une logique de réponse conjointe aux menaces.

Cet effort s'inscrira dans la continuité des partenariats déjà engagés par la France dans des zones de tension informationnelle ou démocratique, notamment dans les Balkans ou en Europe de l'Est et plus largement le voisinage de l'Union européenne.

OBJECTIF STRATÉGIQUE 15. PRIORISER L'ENGAGEMENT DE LA FRANCE DANS LES ENCEINTES MULTILATÉRALES

Faire de la France une voix structurante dans les enceintes multilatérales pour inscrire la LMI dans une vision partagée, fondée sur l'État de droit, la transparence et la résilience démocratique.

La lutte contre les manipulations de l'information ne saurait relever uniquement des politiques nationales. Par définition, les campagnes d'ingérences numériques étrangères impliquent des dynamiques internationales, visent des opinions publiques fragmentées, et s'appuient sur des vecteurs transnationaux. Dans ce contexte, les enceintes multilatérales constituent un levier stratégique essentiel pour faire émerger des normes communes, favoriser la coordination des réponses et porter une vision démocratique de l'espace informationnel mondial.

RENFORCER LA PRÉSENCE ET L'INFLUENCE DE LA FRANCE DANS LES ENCEINTES MULTILATÉRALES

Dans l'Union européenne, la France s'inscrit pleinement dans l'agenda du bouclier démocratique européen, qui repose sur une double logique de résilience interne et d'influence externe. Elle continuera d'appuyer un renforcement du rôle de la Commission européenne et du Service européen pour l'action extérieure dans le suivi, la qualification et la réponse aux campagnes hostiles. Elle proposera notamment une consolidation des canaux de remontée d'informations entre États membres, ainsi qu'une meilleure articulation entre les capacités nationales (de type VIGINUM) et les dispositifs européens de réponse rapide, notamment dans les périodes électorales.

À l'OCDE, la France poursuivra les travaux d'ampleur conduits dans la perspective de renforcer la démocratie ainsi que l'intégrité de l'information. Les recommandations adoptées en la matière le 17 décembre 2024 fournissent un cadre d'action dans lequel il conviendra de s'inscrire.

Au sein du G7, la France continuera de soutenir et contribuer aux mécanismes de coordination politique face aux campagnes informationnelles hostiles, en s'appuyant sur les bonnes pratiques partagées entre membres et des formats d'échanges et de coopérations tels que le *G7 Rapid Response Mechanism*. Ce forum offre une opportunité précieuse pour aligner les doctrines, partager les signaux faibles, harmoniser les pratiques et défendre des principes communs dans une logique de codification et de partage.

À l'ONU, la France portera une voix claire dans les enceintes concernées, notamment l'UNESCO et le Global Digital Compact, pour faire reconnaître les différentes formes de manipulation de l'information comme un terrain d'action multilatéral de première importance tant pour la sécurité, la paix et la démocratie. Elle s'opposera à toute tentative de captation du discours multilatéral par des États autoritaires visant à légitimer la censure ou le contrôle total de l'espace numérique. Elle encouragera, en retour, une reconnaissance des normes démocratiques d'intervention : proportionnalité, redevabilité, droit à l'information, transparence.

Dans le cadre de l'OTAN, la France renforcera sa contribution aux travaux menés sur la réponse aux menaces hybrides. Elle soutiendra notamment les efforts du Centre d'excellence StratCom basé à Riga, tout en promouvant une approche plus offensive dans l'attribution publique et la réponse coordonnée aux campagnes de manipulation menées contre les Alliés.

Affirmant son soutien à un cadre multilatéral fort et efficace, la France continuera de s'investir pleinement dans les enceintes dédiées. La France devra **investir également les enceintes élargies** permettant d'accueillir un dialogue ouvert associant acteurs privés et publics sans pour autant dépendre des choix stratégiques défavorables au multilatéralisme pouvant être opérés par certains États.

Par ailleurs, au sein du monde francophone, **l'organisation internationale de la francophonie** fournit un travail substantiel sur ces sujets et offre ainsi un cadre de partage d'éléments d'information et d'action pertinents qu'il faut pouvoir continuer à investir en lien avec les autres enceintes multilatérales.

Enfin, les manipulations de l'information ne sont pas seulement un enjeu politique ou sécuritaire : elles sont aussi un défi normatif et technique. L'essentiel des règles encadrant l'espace numérique – formats de contenus, chaînes de confiance, protocoles d'authentification, règles de monétisation, structures algorithmiques – est défini dans des enceintes techniques structurantes pour les équilibres informationnels globaux. Dans ces arènes, la France doit défendre une vision fondée sur la transparence, l'éthique de l'ingénierie, la souveraineté numérique et la résilience démocratique.

Par cette stratégie multilatérale, la France entend articuler ses intérêts nationaux et ses principes démocratiques fondamentaux, en contribuant à l'émergence d'un cadre international fondé sur l'intégrité du débat public, la transparence algorithmique, la souveraineté informationnelle des peuples, la transparence et la sécurité partagée.

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