



**COMMISSION D'ENQUÊTE SUR LES POLITIQUES PUBLIQUES FACE AUX
OPÉRATIONS D'INFLUENCES ÉTRANGÈRES VISANT NOTRE VIE
DÉMOCRATIQUE, NOTRE ÉCONOMIE ET LES INTÉRÊTS DE LA FRANCE
SUR LE TERRITOIRE NATIONAL ET À L'ÉTRANGER AFIN DE DOTER
NOTRE LÉGISLATION ET NOS PRATIQUES DE MOYENS D'ENTRAVES
EFFICIENTS POUR CONTRECARRER LES ACTIONS HOSTILES À NOTRE
SOUVERAINETÉ**

**LUTTE CONTRE LES INFLUENCES ÉTRANGÈRES
MALVEILLANTES.
POUR UNE MOBILISATION DE TOUTE LA NATION FACE À
LA NÉO-GUERRE FROIDE.**

Tome 1
Rapport

**M. Dominique de LEGGE
Président**

**M. Rachid TEMAL
Rapporteur**

S O M M A I R E

	<u>Pages</u>
AVANT-PROPOS	11
L'ESSENTIEL.....	17
LES 47 RECOMMANDATIONS DE LA COMMISSION D'ENQUÊTE.....	22
 INTRODUCTION :	
PRÉSENTATION DES PRINCIPALES NOTIONS UTILISÉES ET DES AXES DE	
TRAVAIL DE LA COMMISSION D'ENQUÊTE	
I. LES INFLUENCES ÉTRANGÈRES : DU SOFT POWER AUX MENACES HYBRIDES.....	29
A. L'INFLUENCE, QUI CONSTITUE UNE FINALITÉ NATURELLE ET LÉGITIME DANS LES RELATIONS INTERNATIONALES, SUPPOSE DES STRATÉGIES SPÉCIFIQUES.....	30
1. <i>L'influence, en ce qu'elle s'oppose à la contrainte, constitue une finalité naturelle et reconnue comme légitime dans les relations internationales</i>	30
2. <i>La recherche d'influence suppose des stratégies spécifiques tendant à développer la « puissance douce » et le « pouvoir discursif » des acteurs</i>	32
B. MÊME QUAND ELLE REPOSE SUR DES MOYENS LÉGITIMES, LA RECHERCHE D'INFLUENCE PEUT S'AVÉRER MALVEILLANTE ET APPELER LE CAS ÉCHÉANT DES RÉPONSES DIPLOMATIQUES	33
C. L'INFLUENCE COMPORTE ÉGALEMENT UNE DIMENSION MILITAIRE, EN CE QUE TOUT CONFLIT SE DOUBLE D'UNE « BATAILLE DES PERCEPTIONS »	35
D. L'INFLUENCE PEUT ENFIN ÊTRE RECHERCHÉE PAR LE MOYEN DISSIMULÉ DE L'INGÉRENCE, QUI APPELLE DE MULTIPLES RÉPONSES DE POLITIQUE PUBLIQUE	36
II. UN ANGLE DE TRAVAIL DE LA COMMISSION D'ENQUÊTE AXÉ SUR LES POLITIQUES PUBLIQUES FACE AUX INFLUENCES MALVEILLANTES	41
A. UNE ACTUALISATION DES MENACES PESANT SUR LA FRANCE EN 2024.....	41
B. COMPLÉTER LES TRAVAUX SECTORIELS DES PRÉCÉDENTS RAPPORTS PARLEMENTAIRES PAR UNE APPROCHE GLOBALE DES POLITIQUES PUBLIQUES	42
C. PROPOSER UNE APPROCHE DE LA LUTTE CONTRE LES INFLUENCES ÉTRANGÈRES MALVEILLANTE FONDÉE SUR TROIS PILIERS : SORTIR DE LA NAÏVETÉ, SORTIR DE LA PASSIVITÉ, SORTIR DE L'EMPIRISME	44

PREMIÈRE PARTIE :
LA FRANCE CONFRONTÉE À UN DURCISSEMENT DES STRATÉGIES
D'INFLUENCE

I. LA NOUVELLE DONNE GÉOPOLITIQUE ET TECHNOLOGIQUE : MENACES HYBRIDES ET BATAILLE DES PERCEPTIONS	45
A. UN ENVIRONNEMENT STRATÉGIQUE PLUS COMPLEXE, PLUS INCERTAIN ET PLUS DANGEREUX	45
1. <i>Entre la désinhibition des puissances hostiles et la montée en puissance de l'hybridité sous le seuil de la guerre conventionnelle</i>	45
2. <i>Montée en puissance des menaces hybrides et définition de l'influence comme 6^{ème} fonction stratégique des armées</i>	47
B. PLATEFORMES, INTELLIGENCE ARTIFICIELLE... : DE NOUVEAUX CANAUX DE PERCEPTION DE L'INFORMATION	50
1. <i>La nouvelle donne technique et numérique opère comme un effet multiplicateur des manipulations de l'information</i>	50
2. <i>Guerre informationnelle, bataille des perceptions</i>	51
II. DES COMPÉTITEURS ENGAGÉS DANS UNE GUERRE D'INFLUENCE CONTRE LA FRANCE : CARTOGRAPHIE DE LA MENACE	52
A. À L'INSTAR DES AUTRES PAYS OCCIDENTAUX, LA FRANCE EST PRISE POUR CIBLE PAR LES GRANDES PUISSANCES RÉVISIONNISTES QUE SONT LA RUSSIE ET LA CHINE.....	53
1. <i>La Russie, compétiteur le plus agressif</i>	53
2. <i>La Chine, une menace croissante</i>	56
B. DES MENACES ÉMERGENTES « TOUS AZIMUTS »	59
1. <i>Des compétiteurs étatiques émergents : Azerbaïdjan, Turquie, Iran</i>	59
2. <i>Les influences d'inspiration islamiste : une menace endogène ou d'origine étrangère ?</i>	61
C. QUID DE NOS ALLIÉS ?	63
III. LA FRANCE PRISE POUR CIBLE : INVENTAIRE DE NOS VULÉRABILITÉS	64
A. UNE FRAGILITÉ INHÉRENTE À NOTRE MODÈLE POLITIQUE ET DÉMOCRATIQUE	64
B. UNE EXPOSITION PROPRE À SON STATUT DE SEPTIÈME PUISSANCE MONDIALE	66
C. UNE FRAGILITÉ LIÉE À DES FRACTURES POLITIQUES, SOCIALES ET TERRITORIALES, TERREAU FERTILE AUX INFLUENCES MALVEILLANTES.....	69
D. UNE FRAGILITÉ DÉCOULANT DU DÉSARMEMENT DE L'ÉTAT	72
E. UNE FRAGILITÉ DU CITOYEN	73
1. <i>Une fragilité de l'« individu démocratique »</i>	73
2. <i>La fragilité des décideurs publics et privés</i>	75

IV. LUTTE INFORMATIONNELLE, CAPTURE DES ÉLITES, CONTRÔLE DES DIASPORAS... : TYPOLOGIE DES MODES OPÉRATOIRES	76
A. LES OPÉRATIONS DE LUTTE INFORMATIONNELLE	76
1. <i>Les acteurs de la guerre informationnelle</i>	77
2. <i>L'amplification numérique des opérations de manipulation de l'information</i>	87
B. LES AUTRES TYPES D'OPÉRATIONS D'INFLUENCE.....	100
1. <i>Les opérations visant l'enseignement supérieur et la recherche</i>	100
2. <i>La capture des élites : idiots utiles et trahison des clercs</i>	100
3. <i>Le contrôle et l'instrumentalisation des diasporas et des communautés religieuses.....</i>	102
4. <i>Les opérations d'influence dans le domaine économique</i>	105

DEUXIÈME PARTIE :
UN DISPOSITIF DE PROTECTION ÉTOFFÉ MAIS À GÉOMÉTRIE VARIABLE,
SANS STRATÉGIE D'ENSEMBLE

I. DÉTECTION ET CARACTÉRISATION : UN DISPOSITIF RESSERRÉ AUTOUR DES MINISTÈRES RÉGALIENS.....	109
A. UN PROCESSUS EMPIRIQUE D'ÉLABORATION DES STRATÉGIES SUCCESSIVES DE LUTTE INFORMATIQUE DÉFENSIVE, OFFENSIVE ET INFORMATIONNELLE	109
B. UN TRAVAIL DE DÉTECTION ET DE RIPOSTE DES OPÉRATIONS REPOSANT SUR LA MOBILISATION DE PLUSIEURS ACTEURS	110
1. <i>Viginum, protecteur du débat public numérique national</i>	110
2. <i>La direction de la communication et de la presse : bras armé du Quai d'Orsay pour la veille stratégique.....</i>	114
3. <i>Les armées : une veille constante des menaces informationnelles par le Comcyber et la Dicod</i>	115
4. <i>Les autres « capteurs » : services de renseignement, CIPDR.....</i>	116
C. UN DISPOSITIF DE COORDINATION PILOTÉ PAR LE SGDSN SELON UNE SPÉCIALISATION EN SILO DE L'ORGANISATION DE LA DÉFENSE CONTRE LES ATTAQUES HYBRIDES.....	117
D. UNE COORDINATION HORIZONTALE EFFICACE MAIS RESTREINTE À UN NOMBRE LIMITÉ D'ACTEURS ESSENTIELLEMENT RÉGALIENS : L'EXEMPLE DU COLMI	119
II. RÉPONSE ET RIPOSTE : OUTILS ET LIMITES DU DISPOSITIF ACTUEL.....	120
A. UNE LARGE PALETTE DE MESURES VISANT À ENTRAVER LES OPÉRATIONS D'INFLUENCE.....	120
1. <i>De la divulgation à l'attribution : ébauche d'une communication stratégique à la française</i>	120
2. <i>Les mesures d'entrave dans le champ des armées</i>	124
3. <i>Les actions des services de renseignement.....</i>	129
4. <i>Les actions diplomatiques de nature à faire cesser une opération d'influence</i>	129
5. <i>La saisine de la plateforme Pharos</i>	132
6. <i>L'opportunité de la riposte aux attaques informationnelles d'influence</i>	133

B. LA RÉPRESSION PÉNALE DES OPÉRATIONS D'INFLUENCE	136
1. <i>En l'état du droit, une forte pluralité d'infractions à la disposition de l'autorité judiciaire pour réprimer les actes d'ingérence à visée d'influence</i>	136
2. <i>Un arsenal pénal récemment renforcé par l'adoption de la proposition de loi visant à prévenir les ingérences étrangères en France</i>	143
C. LA POLITIQUE D'INFLUENCE POSITIVE : MAILLON FAIBLE DE LA RÉPONSE FRANÇAISE	147
1. <i>La France pâtit de l'absence d'une véritable politique d'influence</i>	147
2. <i>En dépit d'efforts sectoriels, la France peine à faire émerger une politique d'influence ex nihilo</i>	148
D. LA COORDINATION EUROPÉENNE ET INTERNATIONALE : UNE RÉPONSE EN CONSTRUCTION FACE AUX STRATÉGIES D'INFLUENCE AGRESSIVES	152
1. <i>En matière de communication stratégique et de dénonciation</i>	152
2. <i>La mise en œuvre du régime des mesures restrictives de l'Union européenne comme entrave aux opérations d'influence</i>	158
III. RÉGULATION ET RÉSILIENCE : UNE IMPLICATION INÉGALE DES DIFFÉRENTS ACTEURS DES POLITIQUES PUBLIQUES	160
A. LA RÉGULATION DE L'ESPACE MÉDIATIQUE ET DES PLATEFORMES : DES PROGRÈS IMPORTANTS RÉALISÉS AU COURS DES DERNIÈRES ANNÉES	160
1. <i>Le contrôle des médias étrangers : un renforcement important au cours des dernières années</i>	160
2. <i>La lutte contre les manipulations de l'informations sur les plateformes en ligne : des moyens juridiques renforcés, dans le cadre d'une approche encore trop timorée</i>	164
3. <i>La promotion d'une information de qualité : une responsabilité incombant largement aux médias eux-mêmes, même si l'État peut jouer un rôle d'impulsion et de soutien</i>	176
4. <i>L'enjeu de l'éducation aux médias et à l'information : une prise en compte insuffisante des influences étrangères malveillantes</i>	180
B. LE CONTRÔLE DE LA VIE PUBLIQUE ET POLITIQUE : UN ARSENAL LÉGISLATIF RÉCEMMENT RENFORCÉ, MAIS QUI RESTE À PARFAIRE ET À METTRE PLEINEMENT EN ŒUVRE	183
1. <i>Le financement des campagnes électorales et de la vie politique : un dispositif de contrôle qui comporte encore certaines failles</i>	183
2. <i>Les influences étrangères : un « angle mort » du régime de transparence de la vie publique, corrigé par la récente loi visant à prévenir les ingérences étrangères en France</i>	185
C. L'ENSEIGNEMENT SUPÉRIEUR ET LA RECHERCHE : UNE MISE EN ŒUVRE ENCORE INCOMPLÈTE DES RECOMMANDATIONS DU RAPPORT « GATTOLIN »	192
1. <i>La prise de conscience par le ministère d'un risque d'influences étrangères bien réel</i>	192
2. <i>Un dispositif de protection qui repose sur l'action du service de défense et de sécurité du ministère et le volontarisme des établissements, qui n'est pas encore à la hauteur de la menace</i>	195
3. <i>Un dispositif qui reste marqué par d'importantes lacunes, et en particulier par un défaut d'application des recommandations les plus substantielles du « rapport Gattolin »</i>	204
D. LE CHAMP ÉCONOMIQUE ET INDUSTRIEL : UN ARSENAL LÉGISLATIF RELATIVEMENT COMPLET, MAIS UNE PRISE EN COMPTE ENCORE INSUFFISANTE DES ENJEUX DE SÉCURITÉ INFORMATIONNELLE	211
1. <i>L'action du Sisse, « bras armé du Gouvernement » en matière de sécurité économique</i>	212
2. <i>Les opérations d'influence étrangère : un « angle mort » de la politique de sécurité économique</i>	216

E. LE CHAMP ASSOCIATIF ET CULTUEL : MALGRÉ DES PROGRÈS RÉALISÉS DANS LE CONTRÔLE DU FINANCEMENT ÉTRANGER DES CULTES AINSI QUE DES ÉCOLES PRIVÉES HORS CONTRAT, DES ZONES D'OMBRE SUBSISTENT ...	218
1. <i>Un dispositif de contrôle récemment renforcé par la loi confortant le respect des principes de la République</i>	219
2. <i>Un bilan globalement positif des nouveaux dispositifs issus de la loi confortant le respect des principes de la République, mais des lacunes et des zones d'ombres qui subsistent</i>	224
IV. CONCLUSION INTERMÉDIAIRE : LA NÉCESSITÉ D'UNE STRATÉGIE GLOBALE	228
A. UN BILAN INTERMÉDIAIRE SATISFAISANT : LA FRANCE A CRÉÉ UNE POLITIQUE GLOBALE ET PRIS UNE CERTAINE AVANCE SUR SES PARTENAIRES	228
1. <i>Une approche globale de la lutte contre les influences étrangères qui couvre, en théorie, l'ensemble des politiques publiques</i>	228
2. <i>En comparaison de ses partenaires et alliés, la France dispose d'une certaine avance dans la lutte contre les influences malveillantes</i>	232
B. UN BILAN À PERFECTIONNER : UNE APPROCHE EMPIRIQUE, SANS PORTAGE POLITIQUE INTERMINISTÉRIEL ET INÉGALEMENT MISE EN ŒUVRE SELON LES MINISTÈRES.....	235
1. <i>Une approche de la lutte contre les influences qui frappe par son empirisme</i>	235
2. <i>Un décalage inquiétant entre la sphère régaliennes et le reste des services de l'État sur la prise en compte de la menace des influences malveillantes</i>	236

TROISIÈME PARTIE :

POUR UNE POLITIQUE PUBLIQUE DE LUTTE CONTRE LES INFLUENCES ÉTRANGÈRES MALVEILLANTES FONDÉE SUR TROIS PILIERS

I. LA NÉCESSITÉ DE REFONDER NOTRE APPROCHE COLLECTIVE DU PHÉNOMÈNE	241
A. PREMIER PILIER : SORTIR DE LA NAÏVETÉ, ET ACTER QUE LA LUTTE CONTRE LES INFLUENCES ÉTRANGÈRES MALVEILLANTES EST L'AFFAIRE DE TOUS ..	241
1. <i>À court terme, la nécessité de mesurer l'impact des opérations d'influence étrangères et de nous donner les moyens d'assurer son suivi dans la durée</i>	241
2. <i>À plus long terme, bâtir une société résiliente où chacun se considère acteur de sa protection et de celle des autres</i>	243
B. DEUXIÈME PILIER : SORTIR DE LA PASSIVITÉ, ET ASSUMER UNE VÉRITABLE POLITIQUE D'INFLUENCE AFFIRMATIVE PORTEUSE DE NARRATIFS DÉFENDANT LES VALEURS ET LES INTÉRÊTS FRANÇAIS	246
C. TROISIÈME PILIER : SORTIR DE L'EMPIRISME, ET DOTER L'ÉTAT D'UNE STRATÉGIE GLOBALE, NATIONALE ET INTERMINISTÉRIELLE DONT LA MISE EN ŒUVRE SERAIT ASSURÉE PAR UNE GOUVERNANCE ADAPTÉE	248
1. <i>De multiples initiatives doctrinaires et stratégiques ont été prises dans les années récentes où sont en voie de l'être</i>	248
2. <i>Élaborer une véritable stratégie globale, nationale et interministérielle de lutte contre les influences étrangères</i>	249
3. <i>Mettre en place une gouvernance adaptée</i>	255

II. PREMIER CERCLE : LES MINISTÈRES RÉGALIENS, « NOYAU DUR » DE LA RÉPONSE AUX OPÉRATIONS D'INFLUENCES ÉTRANGÈRES	269
A. LUTTER CONTRE LES INFLUENCES ÉTRANGÈRES SUR LE TERRITOIRE NATIONAL.....	269
1. <i>Renforcer les dispositifs de veille et d'alerte.....</i>	269
2. <i>Améliorer la judiciarisation des opérations d'influence malveillantes en mobilisant pleinement les dispositifs nouvellement adoptés</i>	275
B. DANS LE CHAMP DES ARMÉES, RÉÉVALUER LES MOYENS BUDGÉTAIRES À L'AUNE DES NOUVELLES MENACES.....	276
C. DÉVELOPPER NOTRE INFLUENCE POSITIVE À L'ÉTRANGER EN L'ARTICULANT À LA POLITIQUE DE LUTTE CONTRE LES INFLUENCES MALVEILLANTES.....	278
1. <i>Chef de file de la fonction influence, le ministère de l'Europe et des affaires étrangères doit pouvoir disposer de moyens adéquats en matière de veille et de riposte</i>	278
2. <i>Mobiliser notre audiovisuel extérieur, dans le respect de son indépendance, comme un véritable levier de notre influence positive.....</i>	279
3. <i>Pour construire un récit plus affirmé, notre politique d'influence à l'étranger doit davantage s'appuyer sur les ressources de la société civile</i>	284
D. RENFORCER LES CAPACITÉS COMMUNES DE DÉTECTION ET DE RIPOSTE DE LA FRANCE ET DE SES ALLIÉS	286
1. <i>Porter le sujet des influences auprès de nos alliés</i>	286
2. <i>Soutenir la montée en puissance des capacités de détection et de riposte de nos alliés</i>	288
III. DEUXIÈME CERCLE : LA DIFFUSION D'UNE CULTURE DE LA PROTECTION DANS L'ENSEMBLE DE L'ACTION PUBLIQUE	290
A. LIMITER L'AMPLIFICATION DES OPÉRATIONS D'INFLUENCE DANS LES MÉDIAS ET SUR LES PLATEFORMES	290
1. <i>Renforcer les capacités de contrôle par l'Arcom des médias audiovisuels étrangers.....</i>	290
2. <i>Assumer une politique ambitieuse de régulation de l'espace numérique</i>	292
3. <i>Promouvoir un environnement informationnel de qualité</i>	301
B. RENFORCER LES INSTRUMENTS DE CONTRÔLE DE LA VIE PUBLIQUE ET POLITIQUE À L'AUNE DU RISQUE D'INGÉRENCE	303
1. <i>Combler les lacunes du cadre juridique régissant le financement de la vie politique et donner de nouveaux moyens d'enquête à la CNCCFP</i>	303
2. <i>Donner à la HATVP les moyens de pleinement mettre en œuvre ses nouvelles missions en matière de contrôle des influences étrangères et veiller à préserver le haut niveau d'exigence de ce régime</i>	305
3. <i>Mieux contrôler les risques liés au plus hauts responsables politiques</i>	308
4. <i>Encourager un renforcement les règles déontologiques applicables aux amendements parlementaires</i>	309
C. POURSUIVRE LE RENFORCEMENT DE LA PROTECTION DE L'UNIVERSITÉ ET DE LA RECHERCHE FACE AUX OPÉRATIONS D'INFLUENCE.....	311
D. MAINTENIR UN NIVEAU DE VIGILANCE ÉLEVÉ À L'ÉGARD DES ENJEUX LIÉS AU FINANCEMENT DES CULTES.....	314

IV. TROISIÈME CERCLE: POSER COLLECTIVEMENT LES FONDATIONS D'UNE VÉRITABLE RÉSILIENCE DE LA SOCIÉTÉ	316
A. FINLANDE, ESTONIE ET TAÏWAN: DES EXEMPLES ÉTRANGERS DE RÉSILIENCE COLLECTIVE	316
1. <i>Défense globale et éducation aux médias : le modèle nordique et balte de résilience</i>	316
2. <i>Le principe de réactivité « 2+2+2 » taïwanais : 2 heures, 2 images, 200 mots</i>	319
B. AU TRAVERS D'UNE APPROCHE FONDÉE SUR LA RÉSILIENCE DE LA SOCIÉTÉ FRANÇAISE, CITOYENS ET RESPONSABLES PUBLICS DOIVENT ÊTRE PLUS LARGEMENT SENSIBILISÉS.....	320
1. <i>Soutenir la société civile dans la prise de conscience de l'impératif de sécurité informationnelle</i>	320
2. <i>Sensibiliser plus largement la population face aux risques des influences malveillantes ...</i>	323
ANNEXE :.....	331

**ÉTAT D'APPLICATION DES RECOMMANDATIONS DE LA MISSION
D'INFORMATION DU SÉNAT SUR LES INFLUENCES ÉTATIQUES EXTRA-
EUROPÉENNES DANS LE MONDE UNIVERSITAIRE ET ACADEMIQUE
FRANÇAIS ET LEURS INCIDENCES**

CONTRIBUTION DU GROUPE DE L'UNION CENTRISTE	341
LISTE DES PERSONNES ENTENDUES	347
I. AUDITIONS EN RÉUNION PLÉNIÈRE.....	347
II. AUDITIONS DU RAPPORTEUR.....	351
LISTE DES DÉPLACEMENTS.....	353
TABLEAU DE MISE EN ŒUVRE ET DE SUIVI	357

DOCUMENT PROVOC

DOCUMENT PROVISOIRE

AVANT-PROPOS

*Pas de stratégie sans influence,
pas d'influence sans stratégie.¹*

Thierry Burkhard

Les grands hommes appellent honte le fait de perdre et non celui de tromper pour gagner.

Machiavel, *Histoires Florentines*

La commission d'enquête sur les politiques publiques face aux opérations d'influences étrangères visant notre vie démocratique, notre économie et les intérêts de la France sur le territoire national et à l'étranger afin de doter notre législation et nos pratiques de moyens d'entraves efficents pour contrecarrer les actions hostiles à notre souveraineté a été créée le 1^{er} février 2024 à la demande du groupe socialiste, écologiste et républicain (SER)².

Pourquoi une commission d'enquête sur les influences étrangères ?

Il existe déjà de nombreux travaux parlementaires du Sénat comme de l'Assemblée nationale et de la délégation parlementaire au renseignement (DPR) qui est une instance interparlementaire. Le Sénat s'est plus particulièrement intéressé à la notion d'« influence » sous l'angle des influences étrangères dans les universités³ et des influences chinoises via le réseau Tik Tok⁴. En revanche, c'est le vocable d'« ingérence » qu'ont retenu l'Assemblée nationale⁵ et la DPR⁶ dans leurs travaux, lesquels se sont essentiellement focalisés sur l'identification des menaces dans la vie politique et le monde du renseignement, moins sur les politiques publiques au sens large.

¹ *Revue de la Défense nationale* n° 856 (Janvier 2023)

² [Proposition de résolution n° 242 \(2023-2024\)](#) présentée par Rachid TEMAL et les membres du groupe Socialiste, écologique et républicain.

³ [Rapport d'information n° 873 \(2020-2021\)](#) fait par André Gattolin au nom de la mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences, déposé le 29 septembre 2021.

⁴ [Rapport n° 831 \(2022-2023\)](#) fait par Claude Malhuret au nom de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence, déposé le 4 juillet 2023.

⁵ [Rapport n°1311 \(seizième législature\)](#) fait par Constance Le Grip au nom de la commission d'enquête de l'Assemblée nationale relative aux ingérences politiques, économiques et financières de puissances étrangères – États, organisations, entreprises, groupes d'intérêts, personnes privées – visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français, déposé le 1^{er} juin 2023).

⁶ [Rapport public n° 1454 \(seizième législature- Assemblée nationale\) / n° 810 \(2022-2023 – Sénat\)](#) fait par Sacha Houlié au nom de la délégation parlementaire au renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023, déposé le 29 juin 2023.

La création de la commission d'enquête s'est appuyée sur le constat que **la menace sur le modèle démocratique et les intérêts de la France ne se limite plus ni à la guerre conventionnelle, ni aux ingérences « traditionnelles »** (espionnage, trahison, captation de données, etc.) contre lesquels les services de renseignement luttent par la contre-ingérence. De fait, le départ forcé de la France du Sahel n'est pas un échec militaire mais plutôt l'une des conséquences de la guerre de l'information et de l'influence que livrent des acteurs particulièrement agressifs. Plus largement, **les manipulations de l'information sont devenues un levier pour nuire très concrètement aux intérêts de la France**, dans l'hexagone, comme outre-mer et à l'étranger.

Par son statut de membre du Conseil de sécurité de l'ONU, d'Etat doté de la dissuasion nucléaire, de 7^{ème} puissance économique mondiale et par ses prises de position diplomatiques – notamment sur la guerre en Ukraine ou sur le conflit du Haut-Karabagh – **la France demeure une cible dans le durcissement des relations géopolitiques mondiales**. L'actualité des élections européennes puis des Jeux olympiques place également de la France dans le viseur de puissances étrangères et de groupes para ou non-étatiques malveillants.

Le fait que l'influence soit devenue une fonction stratégique de la revue nationale stratégique 2022 démontre **une prise de conscience récente** – celle d'une menace nouvelle pour nos politiques publiques – qu'il reste à créer et à structurer au travers de nouveaux moyens de « contre-influence », à la différence de la « contre-ingérence » qui relève la mission traditionnelle des services de renseignement.

Les influences étrangères malveillantes au cœur des nouvelles menaces hybrides.

C'est autour de la notion d'**influences étrangères malveillantes** que la commission a identifié le cœur des menaces nouvelles qui s'affranchissent des frontières physiques pour s'attaquer à la vie démocratique de la Nation, à son économie et ses intérêts.

C'est également autour de cette notion que les auditions et les déplacements ont permis de mesurer combien la frontière entre, d'une part, l'influence légitime et le *soft power* et, d'autre part, l'ingérence et la confrontation caractérisée est devenu floue et ténue, dans un continuum que Jean-Yves Le Drian, alors ministre de l'Europe et des affaires étrangères, avait résumé par la formule suivante : « *Il n'y a plus de soft power, il n'y a que du hard power* »¹.

¹ Discours de présentation de la feuille de route de l'influence de la diplomatie française (14 décembre 2021).

Les travaux de la commission d'enquête en quelques chiffres.

Entre le 14 février et le 2 juillet 2024, la commission aura procédé à **46 auditions au total dont 13 à huis clos** pour des raisons de confidentialité des échanges ou de sécurité des personnes entendues. C'est le signe de la sensibilité du sujet, mais aussi une des limites des commissions d'enquêtes dont les pouvoirs s'arrêtent là où commence le secret défense.

Au cours de ces auditions et des cinq déplacements effectués en France et à l'étranger (Bruxelles, Helsinki et Tallinn), **120 personnalités auront été entendues**, dont cinq ministres, des services de l'État, des autorités administratives indépendantes, des organismes européens et internationaux, les principaux réseaux sociaux (Meta, Google, X, Tik Tok), des journalistes, des chercheurs, des experts des médias et de l'intelligence artificielle (IA).

Les auditions publiques de la commission d'enquête auront donné lieu à 125 000 vues sur les réseaux sociaux du Sénat. L'audition la plus suivie aura été celle de Guy-Philippe Goldstein sur l'effet des algorithmes sur la montée des extrêmes, avec 30 000 spectateurs.

Enfin, les outils d'investigation des commissions d'enquête auront été mobilisés tels que l'envoi de questionnaires dont les réponses ont nourri le rapport.

Un défi pour la commission d'enquête : surmonter le double langage et un triple paradoxe.

Volontairement, **la commission ne s'était pas fixée pour but de désigner d'emblée un pays plutôt qu'un autre comme étant à l'origine des menaces**, laissant les personnes entendues répondre spontanément aux questions qu'il s'agisse de la Russie, de la Chine, ou de toute autre partie du monde.

En revanche, l'objectif clairement fixé était de **procéder à une évaluation des politiques publiques dans ce domaine**, en tenant compte d'une spécificité propre aux influences malveillantes : **le double langage** mais aussi **une série de paradoxes**.

Le double langage concerne d'abord celui des puissances étatiques ou des groupes non-étatiques qui profitent des canaux légitimes de communication et de la liberté d'expression des sociétés démocratiques pour diffuser officiellement des mensonges, par exemple sur l'envoi de soldats français en Ukraine, et manipuler l'information à grande échelle. C'est aussi **le double langage des plateformes** et des *Big Tech* dont le discours sur les règles de modération des réseaux sociaux masque certainement un modèle économique opaque et des algorithmes qui survalorisent les prises de positions extrêmes.

Un triple paradoxe a également été identifié.

La question des ingérences étrangères a longtemps été traitée sous l'angle des services de renseignement, avec la discréetion qui les entoure. Or, pour sensibiliser plus largement la sphère de l'action publique, il est nécessaire de sortir de cette culture du secret pour mieux diffuser les messages utiles.

Autre paradoxe, **les influences étrangères malveillantes qui font l'objet d'investissements massifs à l'étranger** (on parle de 1,1 milliard d'euros investis par la Russie dans la propagande, ou encore de 2 millions d'agents en Chine dédiés à la surveillance des réseaux) ne sont traitées en France que par un nombre restreint de services régaliens et une poignée d'experts de la contre-influence, sans véritable synergie avec les médias qui de leur côté consacrent des moyens de plus en plus importants à la vérification de l'information (AFP, les décodeurs, les surligneurs de l'info, etc.)

Le troisième paradoxe est que **chaque citoyen est à la fois la cible et l'acteur** : la cible des influences, positives ou malveillantes, et l'acteur de son libre arbitre. Or, le fait de centraliser la lutte contre les manipulations de l'information ou contre les influences étrangères malveillantes au sein de services étroitement spécialisés ne contribue pas à la sensibilisation de la population. À l'image de la culture de « défense globale » mise en place par les pays nordiques et baltes, il est nécessaire et urgent de bâtir une stratégie de résilience par l'éducation aux médias et la formation de l'esprit critique.

Lutte contre les influences étrangères malveillantes : pour une mobilisation de toute la Nation face à la néo-guerre froide.

Le rapport est constitué de trois parties :

- une première partie consacrée à **une cartographie et une typologie des menaces** auxquelles la France est confrontée en raison du durcissement de l'environnement géopolitique ;

- une deuxième partie sur les politiques publiques, leurs forces et leurs limites, à savoir **un dispositif régalien étoffé, mais à géométrie variable à mesure que l'on s'éloigne du cœur des ministères et services régaliens**, et surtout, sans stratégie globale entre les acteurs publics et les acteurs de la société civile ;

- enfin, une troisième partie destinée à formuler **la principale proposition du rapport**, à savoir **une politique publique de lutte contre les influences étrangères malveillantes**.

La politique publique proposée repose sur trois piliers (construire une stratégie globale et interministérielle pour toute la Nation ; bâtir une dynamique de résilience de la population ; gagner la bataille des narratifs) et **une feuille de route de 47 propositions** à mettre en œuvre dans différents secteurs pour mieux lutter contre les influences étrangères numériques sur le territoire national et pour développer notre influence positive à l'étranger. La

commission a entendu à plusieurs reprise le message selon lequel si on se contente de réagir, on reste toujours en retard. Elle en conclut qu'il faut **réinvestir le champ de la communication et de la bataille des narratifs pour mieux affirmer la voix de la France.**

Ces propositions couvrent également le champ de la **diffusion d'une culture de protection dans l'ensemble de l'action publique et de résilience de la société civile** en abordant les sujets de l'éducation aux médias, de la régulation des plateformes, mais aussi de la protection des universités et le maintien de la vigilance à l'égard du financement des cultes.

Ce rapport a vocation à tirer des conclusions opérationnelles pour une **mobilisation de toute la Nation face à la néo-guerre froide.**

DOCUMENT PROVISOIRE

DOCUMENT PROVISOIRE

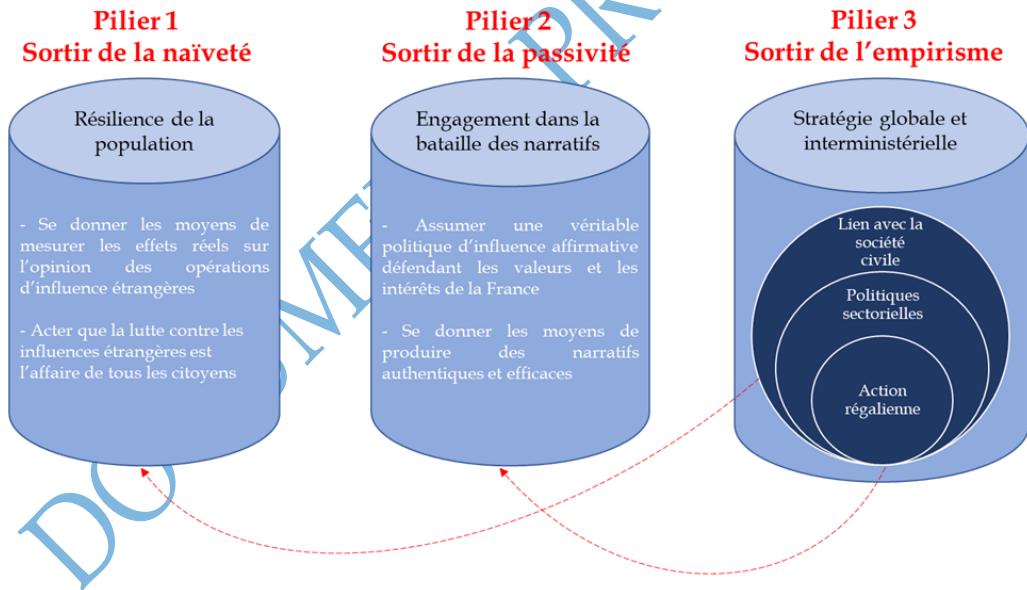
L'ESSENTIEL

Crée à l'initiative du groupe Socialiste, écologiste et républicain (SER), la commission d'enquête sur les politiques publiques face aux opérations d'influences étrangères, présidée par Dominique de Legge (Les Républicains - Ille-et-Vilaine), a adopté le 23 juillet 2024 le rapport présenté par Rachid Temal (SER - Val-d'Oise).

La commission d'enquête propose une politique publique de lutte contre les influences étrangères malveillantes fondée sur trois piliers :

► **une politique publique en 3 piliers** : bâtir une dynamique de résilience de la population ; gagner la bataille des narratifs ; construire une stratégie globale et interministérielle pour toute la Nation.

► **une feuille de route de 47 recommandations** à mettre en œuvre dans différents secteurs pour mieux lutter contre les influences étrangères numériques sur le territoire national et pour développer notre influence positive à l'étranger.



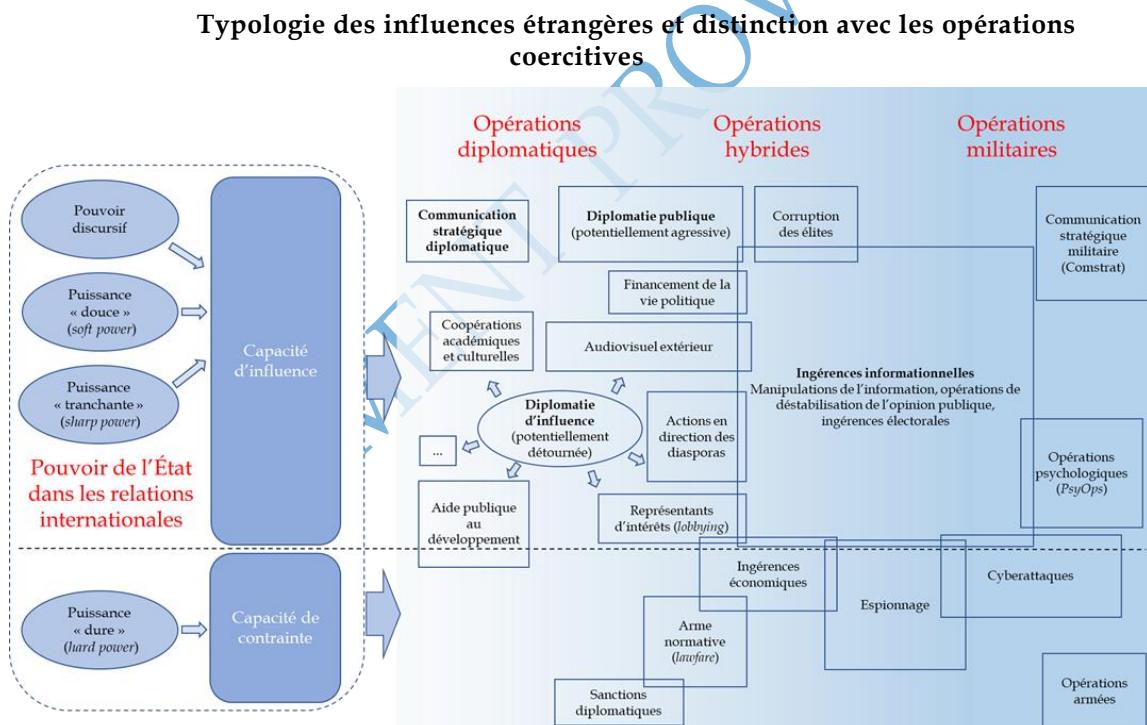
Source : commission d'enquête

I. LES PRINCIPAUX CONSTATS DE LA COMMISSION D'ENQUÊTE

A. LES INFLUENCES ÉTRANGÈRES MALVEILLANTES AU CŒUR DES NOUVELLES MENACES HYBRIDES

La menace sur le modèle démocratique et les intérêts de la France ne se limite plus ni à la guerre conventionnelle, ni aux ingérences « traditionnelles » (espionnage, trahison, *etc.*).

C'est autour de la notion d'influences étrangères malveillantes que la commission d'enquête a centré ses travaux. Cette catégorie se distingue de celle habituellement utilisée de l'« ingérence », qui désigne un moyen plutôt qu'une fin, et est en même temps plus restreinte que celle de l'influence qui, lorsqu'elle est transparente, fait partie du jeu normal des relations internationales. Celles-ci sont assimilables à des attaques hybrides (manipulations de l'information, ingérences numériques étrangères, *etc.*) d'autant plus redoutables qu'elles s'affranchissent des frontières physiques.



Source : commission d'enquête

B. LA FRANCE CONFRONTÉE À UN DURCISSEMENT DES STRATÉGIES D'INFLUENCE

Le recours de plus en plus désinhibé à des stratégies d'influence malveillante contre la France s'inscrit dans un contexte international marqué par :

- **une nouvelle donne géopolitique** avec un retour des stratégies de puissance et une multiplication d'opérations hybrides menées sous le seuil de la guerre conventionnelle ;
- **une nouvelle donne technologique**, caractérisé par la centralité des plateformes numériques et la montée en puissance de l'intelligence artificielle, qui induisent de nouveaux canaux de perception de l'information par les populations.

Plusieurs compétiteurs sont engagés dans une guerre d'influence contre les pays occidentaux et en particulier contre la France : à côté de la Russie - de loin l'acteur le plus agressif et ce dès avant l'invasion de l'Ukraine - et de la Chine, qui s'efforcent de promouvoir leur modèle autoritaire en décrédibilisant la démocratie, des menaces « tous azimuts » se font jour, émanant de compétiteurs étatiques émergents, tels que la Turquie ou l'Azerbaïdjan.

Dans leur guerre d'influence contre la France, nos adversaires exploitent certaines de nos vulnérabilités, qui découlent des fractures bien réelles de notre société, d'un désarmement de l'État dans certains secteurs ou encore également de la fragilité de l'individu et les biais cognitifs dont il peut être victime. **Surtout, ces opérations peuvent paradoxalement tirer profit de notre modèle démocratique et libéral**, caractérisé par un espace informationnel ouvert, qui nous distingue des régimes autoritaires muselant l'opinion publique.

Ces opérations prennent principalement la forme de **manipulation de l'information**. **L'affaire des étoiles bleues de David taguées à Paris** dans les jours qui ont suivi l'attaque du Hamas du 7 octobre 2023 en constitue un prototype : une opération de déstabilisation exploitant un facteur de vive tension politique, portant la signature des services secrets russes, amplifiée artificiellement sur les réseaux sociaux. La typologie des opérations identifiées est cependant plus large : capture des élites, contrôle des diasporas, influence économique etc.

Ces attaques nous placent face à un défi existentiel : celui de ne pas tomber dans le piège qui nous est tendu et donc de refuser, dans notre défense comme dans notre riposte, de céder sur nos principes et nos valeurs démocratiques.

C. UN DISPOSITIF DE PROTECTION ÉTOFFÉ MAIS À GÉOMÉTRIE VARIABLE, SANS STRATÉGIE D'ENSEMBLE

La prise de conscience des stratégies étrangères d'influence malveillantes a conduit à élaborer, bloc par bloc, **un schéma de réponse en trois dimensions** :

- **les actions de détection et de caractérisation**, regroupant les activités de surveillance et d'identification des opérations d'influence. Le

service **Viginum**, placé auprès du Secrétaire général de la défense et de la sécurité nationale (SGDSN), assure ainsi une mission de détection des **ingérences numériques étrangères** (INE) ;

- **les actions de riposte**, correspondant à l'ensemble de la palette d'entraves à la disposition des pouvoirs publics, qui peuvent aller des démarches diplomatiques à une judiciarisation des opérations d'influence. Cet arsenal a récemment été renforcé par la loi « Ingérences étrangères », définitivement adoptée le 5 juin 2024.

- **les politiques de résilience**, visant à protéger la société civile contre les opérations d'influence, en amont de la détection et de la riposte.

Ce schéma de réponse permet de couvrir théoriquement l'ensemble de nos politiques publiques, en permettant de lutter : à l'intérieur, contre **les opérations d'influence visant le territoire national ou l'espace informationnel français** et, à l'extérieur, contre les opérations d'influence ciblant le déploiement et l'image de nos armées ainsi que les intérêts français à l'étranger.

Pour autant et en dépit d'un bilan globalement satisfaisant, **les politiques de lutte contre les opérations d'influences malveillantes frappent par leur empirisme**. La construction de dispositifs *ad hoc* de détection et de caractérisation des actions d'influence malveillante a conduit à une « archipelisation » de nos capacités. Il en découle un **risque de dispersion de nos moyens de réponse**, assorti de l'absence, sur le plan opérationnel, d'une doctrine claire de riposte aux manœuvres hostiles. À ces difficultés opérationnelles s'ajoute **une mauvaise connaissance académique** du phénomène des influences étrangères, peu étudié dans nos universités.

Sur un plan stratégique, **la France ne dispose d'aucune vision unifiée sur la question des influences étrangères malveillantes**. En outre, le sujet ne fait pas l'objet d'un portage politique par le Premier ministre alors qu'il s'agit d'une thématique éminemment interministérielle. Il en ressort **un profond décalage entre l'implication des ministères régaliens, largement mobilisés, et celle des autres administrations**, peu au fait de cette politique. Par ailleurs, la société civile, cible principale des opérations d'influence, est paradoxalement peu associée à la lutte contre cette menace.

II. POUR UNE POLITIQUE PUBLIQUE DE LUTTE CONTRE LES INFLUENCES ÉTRANGÈRES MALVEILLANTES FONDÉE SUR TROIS PILIERS

La commission d'enquête préconise une refonte globale de notre approche collective du phénomène des influences étrangères malveillantes.

• **Premier pilier : bâtir une dynamique de résilience de la population.** À la différence de pays exposés de longue date aux manipulations de l'information, la société française paraît encore trop naïve sur l'état des menaces. Il faut prendre acte que la lutte contre les influences étrangères est l'affaire de tous, les responsables publics comme les citoyens. Elle ne peut pas rester l'apanage de l'État : si les dispositifs de protection, de détection et de riposte que celui-ci met en place sont évidemment nécessaires, ils ne sauraient se substituer à l'effort d'édification d'une société véritablement résiliente.

• **Deuxième pilier : gagner la bataille des narratifs.** La posture défensive, qui a jusqu'ici été la nôtre face aux influences étrangères malveillantes, a montré ses limites. Il est désormais nécessaire d'assumer une véritable politique d'influence positive défendant les valeurs et les intérêts français auprès des opinions publiques internationales, et de s'engager ainsi pleinement dans la bataille des narratifs.

• **Troisième pilier : construire une stratégie globale et interministérielle pour toute la Nation.** Il appartient à l'État de prendre ses responsabilités en se dotant d'une stratégie globale et interministérielle de lutte contre les influences étrangères malveillantes, dans le but d'ordonner son action et ainsi mettre un terme à l'empirisme qui a dominé au cours des dernières années.

Cette stratégie serait structurée en « cercles concentriques », avec un premier volet régional, un deuxième volet dédié aux politiques sectorielles concourant à la lutte contre les influences étrangères malveillantes, et un dernier volet, transversal et inclusif dédié aux actions en direction de la société civile ainsi qu'à l'intégration de ses initiatives, de façon à renforcer notre résilience collective.

Dans ce cadre, la commission d'enquête a formulé 47 recommandations opérationnelles, détaillées *infra*.

LES 47 RECOMMANDATIONS DE LA COMMISSION D'ENQUÊTE

La nécessité de refonder notre approche collective du phénomène

- Recommandation n° 1 : Engager sans délai des recherches académiques transdisciplinaires sur la perception et la réception des opérations de manipulation de l'information sur l'individu et la société, et veiller à l'actualisation régulière de nos connaissances en la matière.
- Recommandation n° 2 : Élaborer une stratégie globale, nationale et interministérielle de lutte contre les influences étrangères malveillantes, en intégrant d'emblée les enjeux de financement et en associant le Parlement. Un débat sur sa mise œuvre se tiendrait annuellement au sein des assemblées.
- Recommandation n° 3 : Établir une doctrine claire en matière de réponse aux opérations d'influence malveillantes.
- Recommandation n° 4 : Conforter Viginum dans son rôle de chef-de-file en matière de protection du débat public numérique, en lui conférant un statut d'agence de l'État dotée d'une autonomie de gestion et placée sous la tutelle du secrétariat général de la défense et de la sécurité nationale (SGDSN).
- Recommandation n° 5 : Réaffirmer le portage politique par le Premier ministre de la politique de lutte contre les influences étrangères malveillantes en la confortant par la désignation d'un membre du Gouvernement placé auprès de lui qui en aurait la charge.
- Recommandation n° 6 : Mettre en place un observatoire des influences étrangères malveillantes regroupant les parties prenantes de la société civile et les acteurs publics concernés.

Lutter contre les influences étrangères malveillantes sur le territoire national

- Recommandation n° 7 : Conférer à Viginum des moyens humains et matériels en adéquation avec sa mission de chef de file en matière de protection du débat public numérique et identifier clairement, au sein des documents budgétaires et dans une logique de transparence, les crédits et les effectifs alloués.
- Recommandation n° 8 : Renforcer les moyens juridiques de Viginum, en : supprimant la référence au seuil des 5 millions de visiteurs uniques par mois pour les plateformes en ligne ; autorisant la collecte automatisée de données dans les activités de veille de Viginum ; allongeant le délai de conservation des données traitées et le délai de renouvellement des collectes ; revoyant la notion d'ingérence numérique étrangère.

• Recommandation n° 9 : Se doter d'un outil de suivi des investissements étrangers en France à l'aune non plus seulement, comme le fait le service de l'information stratégique et de la sécurité économique (Sisse), du caractère stratégique de leur objet mais de leur possible finalité d'influence à moyen-long terme.

• Recommandation n° 10 : Mettre pleinement en œuvre le volet pénal de la loi « Ingérences étrangères », en diffusant largement aux magistrats l'information pertinente sur les nouveaux outils de lutte contre les ingérences étrangères et en intégrant pleinement la caractérisation de la nouvelle circonstance aggravante d'ingérence étrangère dans la coopération entre Pharos et Viginum. Intégrer cette dimension dans la formation des magistrats à l'École nationale de la magistrature.

Dans le champ des armées, réévaluer les moyens budgétaires à l'aune des nouvelles menaces

• Recommandation n° 11 : Réévaluer, à l'occasion de la prochaine actualisation de la loi de programmation militaire, soit avant la fin de l'année 2027, les moyens de la lutte informationnelle à l'aune de l'évolution de la menace.

Développer notre influence positive à l'étranger en l'articulant à la politique de lutte contre les influences malveillantes

• Recommandation n° 12 : Renforcer les dispositifs de veille et d'alerte au sein du ministère de l'Europe et des affaires étrangères, notamment en : développant les capacités de veille et d'enquête en sources ouvertes au sein de la sous-direction « veille et stratégie » de la direction de la presse et de la communication ; poursuivant les efforts de formation du réseau diplomatique aux enjeux de communication stratégique.

• Recommandation n° 13 : Renforcer, dans le cadre du prochain contrat d'objectifs et de moyens, les capacités de France Médias Monde pour lutter contre la désinformation.

• Recommandation n° 14 : Rendre plus accessible les offres de radio de France Médias Monde en langue étrangère sur le territoire français grâce à la radio numérique terrestre (DAB +).

• Recommandation n° 15 : Étendre la diffusion de France 24, notamment en Chine.

• Recommandation n° 16 : Poursuivre les efforts visant à faire d'Arte une « plateforme européenne de référence ».

- Recommandation n° 17 : Créer une « Pléiade d'influence » d'écrivains, scénaristes et représentants des différentes disciplines artistiques au service de la politique d'influence et de la diplomatie publique.

Renforcer les capacités communes de détection et de riposte de la France et de ses alliés

- Recommandation n° 18 : Amplifier l'engagement de la France pour porter l'enjeu de la lutte contre les « FIMI »¹ au niveau de l'Union européenne, de l'Otan, de l'OCDE et du G7, et renforcer les capacités de riposte collectives.
- Recommandation n° 19 : Accompagner les partenaires européens souhaitant se doter de capacités comparables à Viginum.
- Recommandation n° 20 : Accompagner les partenaires de l'Otan souhaitant se doter de capacités comparables à celles du Comcyber.

Limiter l'amplification des opérations d'influence dans les médias et sur les plateformes

- Recommandation n° 21 : Compléter le mandat de l'Arcom pour y intégrer la thématique de la prévention des ingérences étrangères.
- Recommandation n° 22 : Rétablir une obligation de conventionnement avec l'Arcom pour les médias audiovisuels extra-européens.
- Recommandation n° 23 : À l'occasion d'une prochaine révision de la directive « SMA », proposer une simplification de l'application des critères utilisés pour déterminer l'État membre compétent au titre d'un média audiovisuel extra-européen.

¹ Pour Foreign Information Manipulation and Interference, notion développée par le Service européen pour l'action extérieure (SEAE) de l'Union européenne.

• Recommandation n° 24 : Sur le modèle du dispositif prévu à l'article L. 163-2 du code électoral, mettre en place un dispositif permettant à l'autorité judiciaire de faire cesser la diffusion massive et artificielle de contenus faux ou trompeurs rattachables à une ingérence numérique étrangère et de nature à porter atteinte aux intérêts fondamentaux de la Nation.

• Recommandation n° 25 : À court terme, exploiter pleinement les nouvelles prérogatives de régulation conférées par le règlement de l'Union européenne sur les services numériques (DSA) pour s'assurer que les plateformes se donnent les moyens de lutter contre les manipulations de l'information liées à des opérations d'ingérences informationnelles.

• Recommandation n° 26 : À moyen terme, porter au niveau européen une position tendant à conférer aux plateformes un statut d'éditeur au titre d'une partie des contenus qu'ils diffusent ou, a minima, leur conférer un statut hybride d'« entités structurantes de l'espace informationnel » (ni hébergeur, ni éditeur) assorti d'obligations spécifiques permettant de prévenir les ingérences informationnelles.

• Recommandation n° 27 : Se donner les moyens d'une politique industrielle volontariste en faveur de la souveraineté numérique française et européenne, avec pour objectif de long terme que notre espace informationnel cesse d'être structuré par des opérateurs extra-européens.

• Recommandation n° 28 : Identifier spécifiquement les menaces liées aux ingérences étrangères dans les contrats d'objectifs et de moyens passés entre l'État et les médias réalisant des missions d'intérêt général, en prévoyant notamment la mise en place de dispositifs internes de protection sur le modèle de la procédure d'alerte mise en place par France Médias Monde.

Renforcer les instruments de contrôle de la vie publique et politique à l'aune du risque d'ingérence

• Recommandation n° 29 : Combler les lacunes existantes dans le cadre juridique applicable au financement des campagnes électoralles et des partis politiques, en limitant le montant des prêts à un candidat ou à un parti politique, en interdisant aux personnes physiques étrangères ne résidant pas en France de consentir à ce type de prêts, et en interdisant aux mêmes personnes de cotiser aux partis politiques.

• Recommandation n° 30 : Interdire aux partis et aux candidats de recourir aux créateurs de contenus sur les plateformes (« influenceurs ») pour mener des campagnes d'influence électorale rémunérées.

• Recommandation n° 31 : Renforcer les prérogatives de la Commission nationale des comptes de campagnes et des financements politiques (CNCCFP), en lui permettant de demander aux prêteurs d'établir l'origine des fonds prêtés à un candidat ou à un parti politique, d'accéder au

fichier national des comptes bancaires (Ficoba) et en l'intégrant à la liste des personnes à qui Tracfin peut transmettre des informations.

- Recommandation n° 32 : Tirer les conséquences, dans le projet de loi de finances pour 2025, de l'impact de la mise en œuvre de la loi « Ingérences étrangères » sur le budget de la Haute autorité pour la transparence de la vie publique, au regard des nouvelles missions qui lui sont confiées.

- Recommandation n° 33 : Intégrer, dans le rapport au Parlement sur l'état de la menace liée aux ingérences étrangères prévu par la loi « Ingérences étrangères », un premier bilan du fonctionnement de la mise en œuvre du dispositif de contrôle des représentants intérêts agissant pour le compte de mandants étrangers présentant, le cas échéant, les limites rencontrées par la Haute autorité pour la transparence de la vie publique.

- Recommandation n° 34 : Défendre, au niveau européen dans le cadre de la discussion du paquet « défense de la démocratie », un niveau d'exigence en matière de transparence des activités de représentation d'intérêts exercées depuis l'étranger comparable à celui prévu par la loi « Ingérences étrangères ».

- Recommandation n° 35 : Conduire des enquêtes auprès des ministres « pressentis » pour s'assurer de l'absence d'exposition à des influences étrangères.

- Recommandation n° 36 : Encourager résolument en tant que bonne pratique le « sourçage » des amendements et questions parlementaires au Gouvernement lorsqu'ils présentent un lien avec une possible influence étrangère.

Poursuivre le renforcement de la protection de l'université et de la recherche face aux opérations d'influence

- Recommandation n° 37 : Mener un travail de structuration des dispositifs de détection des menaces liées aux influences étrangères au sein des établissements d'enseignement supérieur et de recherche piloté au niveau ministériel, en incluant les établissements privés.

- Recommandation n° 38 : Poursuivre la mise en œuvre des recommandations du « rapport Gattolin », notamment en matière de la protection des sciences humaines et sociales, de contrôle des accords internationaux, et de transparence sur les liens d'intérêts des chercheurs ainsi que sur les financements extra-européens des établissements privés.

- Recommandation n° 39 : Prévoir une procédure d'encadrement systématique des bourses à financement étatique ou para-étatique.

Maintenir un niveau de vigilance élevé à l'égard des enjeux liés au financement des cultes

- Recommandation n° 40 : Combler les lacunes du cadre juridique issu de la loi du 24 août 2021 confortant les principes de la République en matière de contrôle du financement étranger des cultes.

Poser collectivement les fondations d'une véritable résilience de la société

- Recommandation n° 41 : Créer, au sein de Viginum, une nouvelle fonction de sensibilisation et de formation à la sécurité informationnelle, y compris en direction des acteurs privés.
- Recommandation n° 42 : Mener une évaluation exhaustive des dispositifs français d'éducation aux médias et plus largement à l'esprit critique pour consacrer l'éducation aux médias et à l'information comme grande cause nationale, en y intégrant une dimension spécifique aux influences étrangères malveillantes.
- Recommandation n° 43 : Créer un *Pass Médias* pour les jeunes, sur le modèle du *Pass Culture*.
- Recommandation n° 44 : Intégrer dans la Journée défense et citoyenneté une dimension portant sur les influences étrangères.
- Recommandation n° 45 : Créer une spécialité de la réserve opérationnelle et de la réserve citoyenne de défense et de sécurité dédiée à la fonction d'influence et mobilisable pour la détection et la riposte aux opérations d'influence étrangères.
- Recommandation n° 46 : Sensibiliser les élus sur les enjeux liés aux influences étrangères malveillantes (commande publique, cybersécurité etc.).
- Recommandation n° 47 : Examiner la possibilité d'habiliter au secret de la défense nationale davantage de responsables publics, en particulier les exécutifs locaux et les présidents d'établissements d'enseignement supérieur dans la limite du besoin d'en connaître.

INTRODUCTION : PRÉSENTATION DES PRINCIPALES NOTIONS UTILISÉES ET DES AXES DE TRAVAIL DE LA COMMISSION D'ENQUÊTE

I. LES INFLUENCES ÉTRANGÈRES : DU SOFT POWER AUX MENACES HYBRIDES

La notion d'« influence », que l'on a coutume d'associer avec celle de « puissance douce » (*soft power*) et d'opposer à celle d'« ingérence », fait l'objet de riches travaux académiques et de débats de politique publique.

Cet enjeu sémantique et conceptuel est important, en ce qu'il constitue le préalable à la caractérisation adéquate du comportement des acteurs étrangers à l'endroit de la France, de la menace qu'ils représentent, et des **réponses de politique publique** qu'ils appellent, qui constitue **l'objet principal de la commission d'enquête**.

La commission d'enquête s'est par conséquent montrée vigilante à définir précisément les phénomènes à l'œuvre, en veillant à employer les termes adéquats. La plupart des auditions conduites ont abordé cet enjeu.

La présente section introductory détaille donc les différentes définitions et concepts qui seront mobilisés dans la suite du rapport. L'encadré ci-dessous en fait la synthèse.

DOCUMENT confidentiel

Influence, « puissance douce », ingérence... : synthèse des notions

Pour un acteur politique, le fait d'influencer un autre acteur constitue une finalité. **L'influence** figure parmi les finalités naturelles et admises des relations internationales.

La capacité d'influence repose notamment sur le développement de la **puissance douce** (*soft power*) et du **pouvoir discursif** des acteurs. Celle-ci passe notamment par le déploiement des outils de la **diplomatie d'influence** et de la **diplomatie publique** des États, ainsi que leur capacité à mettre en œuvre une **communication stratégique**.

Le caractère naturel et admis de la finalité d'influence et le caractère légitime des leviers diplomatiques mobilisés pour l'atteindre ne signifie pas que l'acteur visé ne doive pas s'en préoccuper. L'influence recherchée peut en effet être malveillante, voire hostile, et appelle des mesures de riposte de nature principalement diplomatique.

Au-delà du champ diplomatique, l'influence comporte également une dimension militaire, et joue un rôle essentiel à chacun des stades du triptyque « compétition - contestation - affrontement » qui structure la doctrine militaire française actuelle.

L'influence malveillante peut également être obtenue par des moyens dissimulés et illégitimes : on parle alors d'**ingérence**. Contrairement à l'influence, l'ingérence n'est pas une finalité mais un procédé : l'influence, même malveillante, peut passer par des canaux légitimes, sans opération d'ingérence : l'inverse, certaines opérations d'ingérence, par exemple dans le champ économique et juridique, relèvent de finalités distinctes de l'influence. Les ingérences à finalité d'influence malveillante, qui passent principalement mais non uniquement par des **opérations de manipulation de l'information**, peuvent, pour le pays qui en est la cible, constituer une **menace dite « hybride »**, et appellent des mesures de défense et de riposte spécifiques, qui excèdent les champs diplomatique ou militaire et concernent de larges pans de politique publique.

Source : commission d'enquête

A. L'INFLUENCE, QUI CONSTITUE UNE FINALITÉ NATURELLE ET LÉGITIME DANS LES RELATIONS INTERNATIONALES, SUPPOSE DES STRATÉGIES SPÉCIFIQUES

1. L'influence, en ce qu'elle s'oppose à la contrainte, constitue une finalité naturelle et reconnue comme légitime dans les relations internationales

L'**influence** peut en première approche faire l'objet d'une définition simple, proposée par le professeur Frédéric Charillon lors de son audition par la commission d'enquête : « *l'influence consiste pour un acteur A à faire faire par un acteur B ce qu'il n'aurait pas fait autrement, et ce, sans recourir à la contrainte* »¹. C'est par ce dernier aspect qu'elle se distingue de la notion de **pouvoir**, dont l'exercice inclut la contrainte ou la menace d'y recourir.

L'influence constitue une finalité naturelle et ancienne dans les relations internationales. Pour autant, elle n'est pas une finalité en soi puisque l'influence n'a d'utilité que si elle est utilisée par un acteur, étatique

¹ Frédéric Charillon, Guerres d'influence. Les États à la conquête des esprits, Odile Jacob, janvier 2022, p. 22.

ou non-étatique, pour défendre ses intérêts. Concrètement, celle-ci permet à un acteur, en fonction de ces intérêts, de « *faire, faire faire, empêcher de faire et refuser de faire* ». Le professeur Charillon fournit à ce titre plusieurs exemples attestant de l'importance stratégique décisive de l'influence pour la France :

- « *faire faire* » : peut être prise en exemple l'opération d'influence menée par les États-Unis pour obtenir en janvier 2021 la dénonciation, par l'Australie, du contrat d'armement passé avec la France pour la livraison de sous-marins nucléaires d'attaque ;

- « *empêcher de faire* » : peut être prise en exemple l'opposition réussie de la France à l'examen en conseil de sécurité des Nations unies d'une résolution approuvant l'intervention des États-Unis en Irak de 2003 ;

- « *faire* » : peut-être prise en exemple la situation où un État convainc un État tiers de lui permettre de survoler son territoire pour faciliter une opération militaire ;

- « *refuser de faire* » : peut être prise en exemple le refus de la France, réitéré à plusieurs reprises au cours de la guerre froide, de voir ses armes nucléaires comptabilisées dans les négociations entre les États-Unis et l'Union soviétique.

En ce qu'elle est exclusive du recours à la force, elle est légitime et admise par le cadre juridique régissant celles-ci depuis la fin de la seconde guerre mondiale, sous l'égide de la Charte des Nations unies.

Ainsi, comme le souligne dans un récent rapport l'Organisation de coopération et de développement économiques (OCDE)¹, « *les entités étrangères, telles que les gouvernements, les organisations politiques ou les entreprises, ont un intérêt légitime à promouvoir et à représenter leurs intérêts dans la société française comme dans d'autres pays* ».

L'OCDE relève que ces pratiques ont généralement trois principaux objectifs :

- influencer les processus décisionnels du pays cible, y compris en influençant les responsables publics et l'opinion publique afin que ceux-ci adoptent des positions favorables aux intérêts de l'entité étrangère ;

- influencer l'image d'une organisation, entreprise ou États étrangers au sein du gouvernement, des médias et de la population d'un autre pays ;

- influencer les orientations de politique extérieure du pays, notamment ses positions dans les négociations internationales.

Selon le même rapport, ces pratiques peuvent même « *constituer une force positive dans les processus de prise de décision publique et, lorsqu'elle implique*

¹ ODCE, « [Renforcer la transparence et l'intégrité des activités d'influence étrangère en France](#) », 22 avril 2023.

des États, constitue un phénomène normal et légitime des relations internationales et de la diplomatie ».

Enfin, comme le présent rapport s'attachera à le montrer (*Première partie, I*), les politiques d'influence tendent à occuper une place croissante dans les relations internationales au cours des dernières années, pour des raisons liées à la fois aux caractéristiques de l'environnement stratégique issu de la fin de la guerre froide et à l'exploitation des possibilités offertes par le numérique dans le champ de l'information et des perceptions.

2. La recherche d'influence suppose des stratégies spécifiques tendant à développer la « puissance douce » et le « pouvoir discursif » des acteurs

Pour développer sa capacité d'influence, un État peut rechercher à accroître sa « puissance douce » (*soft power*), selon le concept forgé par le politologue américain Joseph Nye. Celui-ci peut se définir comme « *la capacité d'influencer les autres afin d'obtenir [d'eux] les résultats souhaités, par l'attraction et la persuasion, plutôt que la coercition et le paiement* »¹. La recherche de puissance douce exclut ainsi la coercition, comme toute politique d'influence, mais également la rémunération, qui peut constituer un levier d'influence distinct (voir *infra*). La notion d'**attraction** est au cœur de la puissance douce qui repose, à titre principal, sur la séduction opérée par le rayonnement d'un modèle culturel et la promotion de certaines valeurs. Il est ici utile de rappeler que le concept de puissance douce a été développé pour décrire la puissance des États-Unis, et le rôle joué à cet égard par la diffusion des valeurs et du « mode de vie » étatsuniens (*American way of life*), diffusés dans le monde entier, notamment au travers des productions hollywoodiennes et des séries télévisées.

Pour autant, la capacité d'influence d'un acteur ne se résume pas à sa puissance douce. L'attraction diffuse exercée par un État sur les populations, sans lien direct avec un objectif stratégique précis, ne garantit pas une adhésion de ces populations et encore moins de leurs gouvernements à sa politique. L'ancien ministre des Affaires étrangères Hubert Védrine, cité par Frédéric Charillon, a rappelé avec humour cet état de fait : « *on peut aimer [l'actrice étatsunienne] Julia Roberts et ne pas aimer [la Secrétaire d'État étatsunienne] Condoleezza Rice* »².

Une autre forme de puissance doit ainsi intervenir : le « **pouvoir discursif** ». Céline Marangé et Maud Quessard, ont défini celui-ci comme « *la capacité pour un État à faire valoir son récit et ses vues politiques et à maîtriser les*

¹ J. S. Nye Jr., « *Soft Power and public diplomacy revisited* » in J. Melissen, J. Wang (dir.), *Debating Public Diplomacy. Now and Next*, Brill Nijhoff, 2019, cité par F. Charillon, op. cit., p. 33.

² Frédéric Charillon, op. cit., p. 37.

discours le concernant sur la scène internationale »¹. Cette capacité est d'autant plus cruciale que, dans le contexte stratégique et technologique mentionné supra, les « guerres d'influence », selon l'expression utilisée par le professeur Charillon, prennent de plus en plus la forme de « guerres de l'information », selon l'expression utilisée tant par Céline Marangé et Maud Quessard, co-auterices, que par David Colon, également auditionné par la commission d'enquête, et selon qui « *en l'espace de quelques années à peine, la puissance des États en est venue à dépendre comme jamais auparavant de leur capacité à recourir à l'information comme à une arme, à des fins militaires, politiques ou diplomatiques* »².

À l'inverse, la capacité de contrainte des autres acteurs, dans les relations internationales, repose sur la « **puissance dure** » (*hard power*), qui découle elle-même principalement de la puissance militaire, économique et technologique d'un État.

B. MÊME QUAND ELLE REPOSE SUR DES MOYENS LÉGITIMES, LA RECHERCHE D'INFLUENCE PEUT S'AVÉRER MALVEILLANTE ET APPELER LE CAS ÉCHÉANT DES RÉPONSES DIPLOMATIQUES

Pour accroître sa puissance douce, son pouvoir discursif et, *in fine*, sa capacité d'influence, les États recourent traditionnellement aux outils traditionnels de la diplomatie d'influence et de la diplomatie publique.

La **diplomatie d'influence** regroupe un ensemble d'actions concourant au développement du potentiel d'attraction et donc de la puissance douce d'un État. Dans le cas de la France, celle-ci passe notamment par l'action en faveur des droits de l'Homme, l'action culturelle, *via* les Instituts français notamment, l'aide publique au développement (APD) ou encore le développement de la Francophonie.

La **diplomatie publique** est celle qui s'adresse aux populations des États dans laquelle elle se déploie. Elle se matérialise, selon la définition qu'en donne Frédéric Charillon, par un ensemble d'actions « *consistant à la fois à promouvoir publiquement le contenu de la diplomatie d'État, et à prendre contact directement avec des publics, sans passer par leurs autorités politiques* »³.

La diplomatie d'influence et la diplomatie publique peuvent passer par des actions diverses déployées dans une multitude de champs. Elles investissent ainsi notamment :

¹ Céline Marangé et Maud Quessard (dir.), *Les guerres de l'information à l'ère numérique*, Presses universitaires de France, janvier 2021, p. 13.

² David Colon, *La guerre de l'information. Les États à la conquête de nos esprits*, Taillandier, septembre 2023, p. 11.

³ Frédéric Charillon, « *Chapitre IV. Les politiques d'influence* », Maurice Vaïsse éd., *Diplomatie française. Outils et acteurs depuis 1980*, Odile Jacob, 2018, pp. 381-394.

- le **champ médiatique**, avec notamment le développement de médias internationaux. L'audiovisuel extérieur, reposant sur France Médias Monde, constitue un outil important du dispositif français de diplomatie publique ;

- la **vie publique**, notamment via le recours à des représentants d'intérêt (*lobbying*) rémunérés ou le soutien à des laboratoires d'idées (*think tanks*) ;

- les **champs culturel et académique**, notamment *via* le développement de partenariats, de coopérations et d'échanges ;

- les **champs associatif et cultuel**, *via* le soutien ou la communication réalisés auprès des associations ou des cultes, en particulier lorsqu'ils impliquent des ressortissants de l'État concernés ou leurs descendants résidant dans un État étranger (diaspora).

Le pouvoir discursif passe également par la capacité d'un État à mettre en œuvre une **communication stratégique**, qui peut se définir comme « une communication mise au service des objectifs stratégiques d'un État »¹. Son efficacité dépend de la capacité de l'État à produire un récit (ou un « narratif ») parvenant à présenter de manière positive, de façon structurée et adaptée au public qu'il cible, les valeurs et les intérêts qu'il défend ainsi que la cohérence de son action internationale au regard de ses valeurs et de ses intérêts. Les grandes plateformes numériques (X, Instagram, Facebook, Youtube...) sont devenus des canaux privilégiés de la communication stratégique des États.

L'ensemble de ces leviers peuvent être mis au service d'une influence que l'on peut qualifier de « positive », qui vise à défendre ses intérêts sans chercher à nuire ou à affaiblir un autre État.

Cela étant, ces mêmes outils peuvent être mis au service d'une posture agressive sur la scène internationale. Le cas de l'évolution de la diplomatie chinoise, présenté *infra* (*Première partie, III*), en constitue une illustration.

À cet égard, il convient de relever **qu'une opération d'influence malveillante menée contre un pays donné peut aussi bien cibler directement l'opinion publique de ce pays, mais également avoir pour objet de porter atteinte à ses intérêts à l'étranger en ciblant les opinions publiques de pays tiers**. L'exemple de campagnes de désinformation menées contre la France en Afrique, par la Russie notamment, en est l'illustration (voir *Première partie, IV*).

Cependant, dès lors que les outils mobilisés appartiennent au champ des outils traditionnels de la diplomatie d'influence et de la diplomatie publique et sont utilisés de façon transparente, sans recourir à l'ingérence (voir *infra*), **la riposte, le cas échéant, ne peut qu'être de nature diplomatique**.

¹ David Colon, op. cit., p. 455.

C. L'INFLUENCE COMPORTE ÉGALEMENT UNE DIMENSION MILITAIRE, EN CE QUE TOUT CONFLIT SE DOUBLE D'UNE « BATAILLE DES PERCEPTIONS »

Au-delà du champ diplomatique, l'influence intervient également dans le champ militaire.

Comme le précisent les éléments publics de doctrine du ministère des armées en matière de lutte informatique d'influence (L2I), « *la guerre de l'information est partie intégrante de toute stratégie militaire : sans capacité à convaincre et à contrer l'influence adverse, tout engagement militaire est voué à l'échec.* »¹

L'influence intervient à chacun des stades du triptyque « compétition – contestation – affrontement » qui structure la stratégie militaire française². Celle-ci, en effet, pose avec force l'objectif de « *gagner la guerre avant la guerre* », et confère à ce titre un rôle décisif à la « *bataille des perceptions* »³.

Comme l'a rappelé devant la commission d'enquête le général Pascal Ianni, directeur du pôle « anticipation stratégique et orientations » (ASO) à l'état-major des armées, sous le seuil de l'engagement armé, « *l'arme informationnelle (...) attribuable ou non, assumable ou non, est l'expression même de la compétition, de la contestation et de l'affrontement* »⁴.

Dans le cadre d'un conflit armé, la lutte d'influence se déploie essentiellement dans la couche informationnelle du cyberspace, notamment sur les grandes plateformes numériques. Elle se matérialise notamment par la communication stratégique militaire (ComStrat) ciblant l'opinion publique locale du théâtre d'opération ou l'opinion publique internationale, ainsi que par la conduite d'opérations psychologiques (dites « PsyOps »), qui peuvent être définies comme des opérations menées « *pour influencer les opinions, les émotions, les motivations et les comportements des troupes ennemis ou des civils, de sorte à perturber les prises de décision de l'adversaire* »⁵.

Le ministère souligne le caractère critique de la lutte d'influence dans ce contexte : « *l'extension du combat de l'information vers le cyberspace est un générateur d'instabilité dans l'environnement des opérations militaires. Elle fait peser au quotidien des risques sur les forces armées et peut compromettre leurs chances de succès* ». Ainsi, « *la conquête, puis la maîtrise de la supériorité dans le champ informationnel, sont devenues des conditions de la supériorité opérationnelle* »⁶.

¹ Ministère des armées, [Éléments publics de doctrine militaire de lutte informatique d'influence \(L2I\)](#), octobre 2021.

² [Vision stratégique du chef d'état-major des armées](#), octobre 2021.

³ [Revue nationale stratégique 2022](#).

⁴ [Audition](#) du 2 mai 2024.

⁵ David Colon, op. cit., p. 455.

⁶ Ministère des armées, [Éléments publics de doctrine militaire de lutte informatique d'influence \(L2I\)](#), octobre 2021.

D. L'INFLUENCE PEUT ENFIN ÊTRE RECHERCHÉE PAR LE MOYEN DISSIMULÉ DE L'INGÉRENCE, QUI APPELLE DE MULTIPLES RÉPONSES DE POLITIQUE PUBLIQUE

L'influence malveillante peut également être obtenue par des moyens dissimulés et illégitimes : on parle alors **d'ingérence**.

Les opérations d'ingérence sont définies par l'OCDE¹ comme des « *actions intentionnelles d'acteurs étatiques ou non-étatiques conduites dans l'intérêt d'un gouvernement étranger* », étant précisé que « *ces actions sont secrètes, non-transparentes ou de nature manipulatrice et visent à impacter négativement les structures ou les processus du système politique, l'économie, la société ou l'espace informationnel* ». Sont donc exclues du champ de cette définition « *les opérations cinétiques, telles que les attaques de sabotage, les assassinats ciblés et les actions terroristes, ainsi que les opérations militaires manifestes ou secrètes* ».

L'OCDE indique également que **cette définition des actions d'ingérence est par essence d'inspiration démocratique, en ce qu'elle insiste sur « l'impact négatif sur le pays cible et son fonctionnement d'État souverain démocratique** ». Elle se distingue ainsi de la conception que s'en font les régimes autoritaires, qui tendent à considérer toute action étrangère sur son territoire comme une ingérence, indépendamment de son caractère malveillant. L'OCDE prend en exemple « *la loi relative aux agents étrangers en Russie vise principalement les organisations, notamment celles de la société civile, qui reçoivent un financement de l'étranger, ce qui suffit à les caractériser comme agents de l'étranger, avec des conséquences civiles et pénales pour ces organisations et leurs personnels* ».

Contrairement à l'influence, l'ingérence n'est pas une finalité mais un procédé : l'influence, même malveillante, peut passer par des canaux légitimes, sans opération d'ingérence ; à l'inverse, certaines opérations d'ingérence, par exemple dans le champ économique et juridique, relèvent de finalités distinctes de l'influence.

Les ingérences à finalité d'influence malveillante sont principalement de nature informationnelle. Il s'agit d'opérations de manipulation de l'information et de déstabilisation des opinions publiques.

Pour les caractériser, les institutions de l'Union européenne se réfèrent à la notion de *Foreign interference and manipulation of information (FIMI)*. Le Service européen pour l'action extérieure (SEAE), qui a élaboré cette définition en 2021, présente ces actions comme un ensemble de comportements, majoritairement non illégaux, qui menacent ou ont le potentiel d'affecter négativement les valeurs et le processus politiques. Ces activités à dessein de manipulation sont conduites de manière coordonnée et intentionnelle par des acteurs étatiques ou non étatiques, dont des *proxies*.

¹ ODCE, [« Renforcer la transparence et l'intégrité des activités d'influence étrangère en France »](#), 22 avril 2024.

Le droit français permet également de caractériser les opérations de manipulation de l'information dans le domaine numérique comme des « **ingérences numériques étrangères** » (INE)¹. Celles-ci sont ainsi définies comme des : « *opérations impliquant, de manière directe ou indirecte, un État étranger ou une entité non étatique étrangère, et visant à la diffusion artificielle ou automatisée, massive et délibérée, par le biais d'un service de communication au public en ligne, d'allégations ou imputations de faits manifestement inexacts ou trompeuses de nature à porter atteinte aux intérêts fondamentaux de la Nation* ».

Ces deux définitions permettent d'identifier trois caractéristiques principales des opérations de manipulation de l'information en ligne, réalisées par des entités étrangères, étatiques ou non :

- une diffusion artificielle ou automatisée, massive et délibérée ;
- un contenu reposant sur des informations fausses ou trompeuses ;
- une atteinte aux intérêts de l'État visé.

La conduite de telles opérations témoignerait d'une « puissance tranchante » (*sharp power*) des États qui les maîtrisent, selon la notion popularisée en 2017 par deux chercheurs américains², et définie par le professeur Colon comme « *la politique manipulatrice des régimes autoritaires qui pénètrent et perforent les environnements politiques et informationnels des États démocratiques dans le but d'influencer et de saper leur pouvoir politique* »³. Par construction, la menace représentée par les manipulations de l'information revêt ainsi une dimension critique dans un contexte électoral.

Les travaux de l'OCDE mettent en avant plusieurs autres formes d'ingérence à finalité d'influence, telles que :

- la capture **des élites politiques et économiques**, notamment par le levier de la corruption ;
- le **financement de la vie politique** ;
- une **utilisation détournée de la diplomatie d'influence**, qui peut être caractérisée notamment par l'utilisation abusive de la coopération universitaire, culturelle, des organisations de la société civile et des laboratoires d'idées ou encore par une action de contrôle et de surveillance, voire de répression transnationale, des diasporas.

Du point de vue de la défense et de la sécurité nationale, de telles opérations d'ingérence se rattachent à la catégorie des « **stratégies hybrides** », définies par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) comme « *le recours par un acteur étatique ou non à une combinaison intégrée et volontairement ambiguë de modes d'actions militaires et non militaires* »,

¹ Article R. 1132-3 du code de la défense.

² C. Walker, J. Ludwig, « The Meaning of sharp power : How authoritarian States project influence », Foreign Affairs, 16 novembre 2017.

³ David Colon, op. cit., p. 455.

directs et indirects, légaux ou illégaux, difficilement attribuables. Jouant avec les seuils estimés de riposte et de conflit armé, cette combinaison est conçue pour contraindre et affaiblir l'adversaire, voire créer chez lui un effet de sidération ».

Les domaines concernés par les stratégies hybrides

Le *Cadre conceptuel sur les menaces hybrides*¹, élaboré en 2021 sous l'égide de la **commission européenne et de l'Otan**, identifie **treize domaines** dans lesquels des stratégies hybrides sont susceptibles de se déployer : les infrastructures, le cyber, l'espace, l'économie, le domaine militaire, la culture, le social, l'administration publique, le droit, l'espionnage, la diplomatie, le domaine politique et l'information.

Sur cette base, le **Secrétariat général de la défense et de la sécurité nationale** a identifié précisément **cinq domaines d'action prioritaires pour la France** :

- le cyber et la protection contre les cyberattaques ;
- le champ informationnel et la lutte contre les manipulations de l'information ;
- l'utilisation de l'arme normative (*lawfare*), en particulier dans le cadre de stratégies d'affaiblissement des normes internationales et du recours croissant à des dispositifs juridiques extraterritoriaux ;
- la sécurité économique, qui vise la promotion des intérêts économiques, industriels et scientifiques de la Nation, constitués notamment des actifs matériels et immatériels stratégiques pour l'économie française, ainsi que la défense de la souveraineté numérique ;
- le champ opérationnel militaire.

Source : commission d'enquête

Le champ de la définition des stratégies hybrides, qui englobe le recours à la puissance « dure » avec une finalité de contrainte, excède donc le champ de l'influence.

Toutefois, à l'instar de l'absence de frontière exacte entre influence et ingérence, la notion d'influence malveillante se situant dans un intervalle mouvant, au moins trois domaines ont donné lieu à un questionnement plus particulier : l'utilisation de l'arme normative (*lawfare*), la sécurité économique et la cybersécurité.

À titre d'exemple, l'utilisation de l'arme normative (*lawfare*) mobilise des ressources de puissance « dure » - la capacité d'un État à imposer ses dispositifs juridiques en découlant - et poursuit une finalité de contrainte, même s'il ne s'agit que d'une contrainte juridique, généralement recherchée dans le domaine économique. Elle ne relève pas *stricto sensu* d'une stratégie d'influence.

¹ Centre commun de recherche (JRC) de la commission européenne, et Centre d'excellence d'Helsinki en matière de lutte contre les menaces hybrides (Hybrid COE), [The Landscape of Hybrid Threats : A Conceptual Model](#) (public version), 2021.

La sécurité économique, et l'enjeu de protection de nos actifs, technologies et données stratégiques, qui sont des attributs de puissance « dure », ne relèvent en général pas de la guerre d'influence. Les opérations d'influence constituent cependant bien l'un des trois piliers de l'intelligence économique¹. De telles opérations « visent à convaincre, séduire ou dissuader les organismes décideurs évoluant dans l'environnement direct d'une entreprise »². En particulier, l'atteinte réputationnelle qui pourrait être portée à des entreprises françaises dans le cadre de manipulations de l'information peut relever à la fois de la guerre économique et de la guerre d'influence menées, simultanément contre les entreprises concernées pour des raisons économiques et contre la France pour des raisons politiques.

De même, les cyberattaques ciblant les réseaux informatiques et les systèmes d'informations, en ce qu'elles font appel à des moyens technologiques, ne relèvent pas directement de l'influence. Du point de vue du ministère des armées, la lutte contre les cyberattaques fait d'ailleurs l'objet d'une doctrine distincte de celle de la L2I, mentionnée *supra* : la politique de lutte informatique défensive (LID)³. Les cyberattaques peuvent cependant être mobilisées en tant que pièce d'une opération d'ingérence informationnelle plus large, par exemple :

- dans le cadre d'une opération de « piratage et fuite de données » (*hack and leak*), en intégrant aux fuites réelles des éléments de désinformation destinés à déstabiliser l'opinion publique, telle que la campagne des « *Macron Leaks* » menée en France durant les élections présidentielles de 2017 (voir *Première partie, IV*) ;

- dans le cadre d'une opération de manipulation de l'information tendant à diffuser de façon massive des contenus relatifs à une cyberattaque particulière dans le but d'afficher la prétendue faiblesse de l'État, ou de l'entreprise, qui en a été la cible.

Il résulte de tout ce qui précède que la lutte contre les influences étrangères malveillantes, en particulier lorsqu'elles prennent la forme d'ingérences appelle des mesures de défense et de riposte spécifiques, qui excèdent les champs diplomatique ou militaire pour embrasser de larges pans de politiques publiques, que le présent rapport s'attachera à examiner : régulation des plateformes numériques et des médias, régulation de la vie

¹*L'intelligence économique peut se définir comme « l'ensemble des actions coordonnées de recherche, de traitement et de distribution en vue de son exploitation, de l'information utile aux acteurs économiques. Ces diverses actions sont menées légalement avec toutes les garanties de protection nécessaires à la préservation du patrimoine de l'entreprise, dans les meilleures conditions de qualité, de délais et de coût »* (source : [Rapport](#) du Groupe « Intelligence économique et stratégie des entreprises » du Commissariat général au Plan présidé par Henri Martre, février 1994).

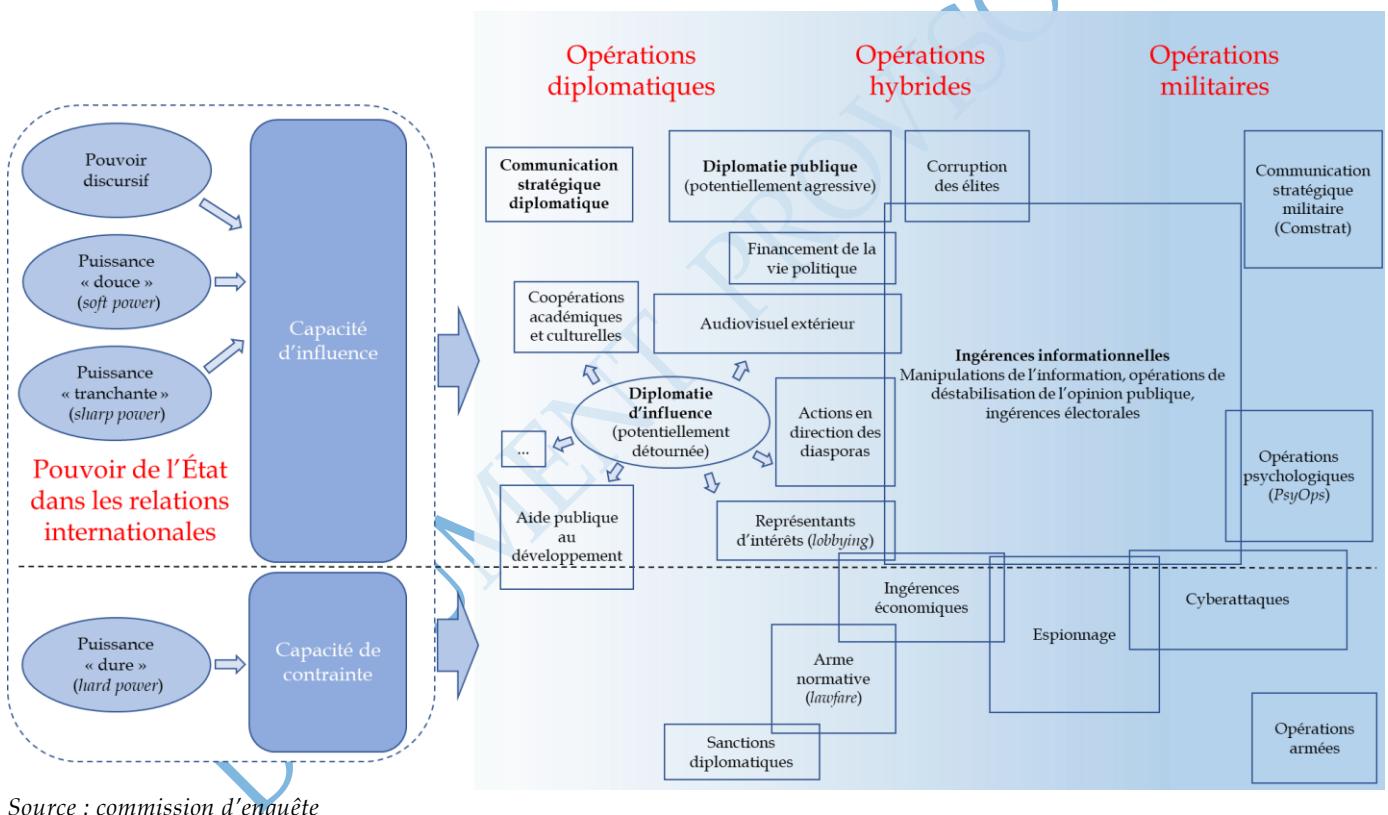
² [Rapport d'information n° 872 \(2022-2023\)](#) fait par Marie-Noëlle Lienemann et Jean-Baptiste Lemoyne au nom de la commission des affaires économiques du Sénat sur l'intelligence économique, déposé le 12 juillet 2023.

³ Ministère des armées, [Politique ministérielle de lutte informatique défensive](#).

politique et économique, politique pénale, enseignement supérieur et recherche, financement des associations et des cultes, éducation nationale...

Pour conduire l'ensemble de ces politiques, une démocratie comme la France est placée face à l'exigence de rester fidèle à ses valeurs, sans quoi l'objectif visé par les opérations d'influence de ses compétiteurs, qui est précisément de les saper, serait en réalité atteint. La guerre d'influence à l'œuvre, qui sera détaillée dans le présent rapport, est en effet un conflit essentiellement asymétrique, dans le cadre duquel des États autoritaires s'ingèrent dans les espaces informationnels ouverts d'États démocratiques pour y manipuler l'information, tout en contrôlant fermement leur propre espace informationnel.

Principales opérations d'influence étrangères et distinction avec les opérations coercitives



II. UN ANGLE DE TRAVAIL DE LA COMMISSION D'ENQUÊTE AXÉ SUR LES POLITIQUES PUBLIQUES FACE AUX INFLUENCES MALVEILLANTES

Le travail de définition préalable de la notion d'influence a constitué la première étape des travaux de la commission afin de resserrer les investigations de la commission d'enquête autour de l'évaluation des politiques publiques, à travers une cartographie des menaces et une typologie des modes d'actions. Il s'agissait de proposer une stratégie globale de lutte contre les influences étrangères malveillantes, dans une approche prospective incluant le développement de technologies nouvelles ou de rupture (algorithmes, intelligence artificielle, informatique en nuage, souveraineté numérique, etc.).

A. UNE ACTUALISATION DES MENACES PESANT SUR LA FRANCE EN 2024

La proposition de résolution n° 242 (2023-2024) présentée par M. Rachid Temal et les membres du groupe Socialiste, écologiste et républicain (SER) retient la notion d'influence en ce qu'elle reflète l'évolution de ce qui recouvre la guerre de l'information dont les effets ont pu être documentés en Afrique contre les intérêts français et en Europe orientale, à partir de la Russie, contre plus généralement le modèle démocratique occidental.

Ce sujet, partiellement défriché par des chercheurs mais aussi des travaux parlementaires (voir *infra*), a fait l'objet de plusieurs auditions afin d'actualiser les constats au contexte très particulier des menaces pesant sur la France en 2024 :

- le retrait récent du Sahel ;
- l'aide fournie par la France à l'Ukraine ;
- la position de la France quant à la guerre Israël-Hamas et le programme nucléaire iranien ;
- les tensions croissantes en Indopacifique (mer rouge, Taïwan) qui ouvrent le champ à des influences étrangères remettant en cause la légitimité de la France dans certains territoires ultramarins ;
- les élections européennes ;
- enfin, l'organisation des jeux Olympiques et Paralympiques de Paris ;

Considérant que les influences étrangères concourent à l'émergence des guerres dites « hybrides » qui demeurent sous le seuil de la conflictualité conventionnelle - médias, manipulation de l'information, cyberspace et dès à présent l'usage croissant de l'intelligence artificielle (IA) - la commission a

consacré une large part de ses auditions et tables rondes à la présentation par des chercheurs d'études scientifiques et prospectives sur les menaces et les moyens d'y répondre.

B. COMPLÉTER LES TRAVAUX SECTORIELS DES PRÉCÉDENTS RAPPORTS PARLEMENTAIRES PAR UNE APPROCHE GLOBALE DES POLITIQUES PUBLIQUES

Les travaux parlementaires et académiques récents ont principalement dressé un état des lieux des politiques d'influence auxquels la France et l'Union européenne font face essentiellement sous un angle sectoriel.

On peut ainsi relever par ordre chronologique deux rapports sénatoriaux :

- la mission d'information « Gattolin » sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences (juillet 2021)¹ ;

- la commission d'enquête « Malhuret » sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence (juillet 2023)².

À l'Assemblée nationale, une commission d'enquête a porté sur les ingérences politiques, économiques et financières de puissances étrangères - États, organisations, entreprises, groupes d'intérêts, personnes privées - visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques (juin 2023). Force est toutefois de constater que les travaux de cette commission, issus d'un « droit de tirage » du groupe Rassemblement national (RN), avaient été fortement perturbés par les désaccords et les mises en cause politiques réciproques de son président (RN) et de sa rapporteure (Renaissance)³.

Enfin la délégation parlementaire au renseignement a consacré ses travaux de la session 2022-2023 aux ingérences étrangères sous l'angle plus spécifique des services de renseignement (juin 2023)⁴.

¹ [Rapport d'information n° 873 \(2020-2021\)](#) fait par André Gattolin au nom de la mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences, déposé le 29 septembre 2021.

² [Rapport n° 831 \(2022-2023\)](#) fait par Claude Malhuret au nom de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence, déposé le 4 juillet 2023.

³ [Rapport n°1311 \(seizième législature\)](#) fait par Constance Le Grip au nom de la commission d'enquête de l'Assemblée nationale relative aux ingérences politiques, économiques et financières de puissances étrangères - États, organisations, entreprises, groupes d'intérêts, personnes privées - visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français, déposé le 1^{er} juin 2023, Tome I.

⁴ [Rapport public n° 1454 \(seizième législature- Assemblée nationale\) / n° 810 \(2022-2023 - Sénat\)](#) fait par Sacha Houlié au nom de la délégation parlementaire au renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023, déposé le 29 juin 2023.

Au niveau européen on relève deux rapports notables :

- le Service européen pour l'action extérieure (SEAE) a publié en février 2023 et en janvier 2024 un rapport sur les manipulations d'information et les ingérences étrangères en Europe¹ ;

- au Parlement européen, une commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation a été créée en 2020, et présidée par Raphaël Glucksmann, qui a publié plusieurs rapports de sa rapporteure Sandra Kalniete², ainsi que de ses corapporteurs Vladimír Bilčík et Nathalie Loiseau sur la question spécifique des recommandations pour la réforme des règles du Parlement européen en matière de transparence, d'intégrité, de responsabilité et de lutte contre la corruption³.

Ces différents rapports partagent le constat d'un durcissement des stratégies d'influence de certains pays depuis les années 2000. Il s'agit en particulier de la Russie et de la Chine, qui ont renforcé leurs diplomatisies culturelles dans la perspective d'une confrontation avec le modèle libéral qualifié d'« occidental » par ces deux pays. Ils s'appuient sur différents canaux d'influence, sur les plans médiatiques, économiques et universitaires.

Au-delà de ces exemples topiques, d'autres États, comme la Turquie ou les pays du Golfe, s'inscrivent également dans des stratégies d'influence plus agressives. En outre, des États alliés, à l'instar des États-Unis, ont recours à des politiques d'influence qui peuvent ne pas être alignés avec nos intérêts, particulièrement dans la sphère économique.

Néanmoins, ces travaux se sont principalement concentrés sur le concept d'ingérence et n'ont abordé que partiellement la notion d'influence, soit en se concentrant sur la politique d'un seul État, soit en étudiant un aspect sectoriel des politiques d'influence.

Globalement, à l'exception du rapport « Gattolin » précité dans le secteur de l'enseignement supérieur, ces rapports ont davantage porté sur

¹ Service européen d'action extérieure, [1^{er} rapport sur les manipulations de l'informations et ingérences étrangères \(FIMI\)](#) (février 2023) et [2^{ème} rapport](#) (janvier 2024) -consultables en anglais.

² [Rapport A9-0022/2022](#) fait par Sandra Kalniete au nom de la Commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (INGE 1) (2020/2268(INI)), 8 février 2022 ; [Rapport A9-0187/2023](#) fait par Sandra Kalniete au nom de la Commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (INGE 2) (2022/2075(INI)), 15 mai 2023.

³ [Rapport A9-0215/2023](#) sur des recommandations pour la réforme des règles du Parlement européen en matière de transparence, d'intégrité, de responsabilité et de lutte contre la corruption (2023/2034(INI)) fait par Vladimír Bilčík et Nathalie Loiseau au nom de la Commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation, et sur le renforcement de l'intégrité, de la transparence et de la responsabilité au Parlement européen, 13 juin 2023.

l'identification des menaces elles-mêmes que sur les politiques publiques à même d'y faire face.

C. PROPOSER UNE APPROCHE DE LA LUTTE CONTRE LES INFLUENCES ÉTRANGÈRES MALVEILLANTE FONDÉE SUR TROIS PILIERS : SORTIR DE LA NAÏVETÉ, SORTIR DE LA PASSIVITÉ, SORTIR DE L'EMPIRISME

Dans le souci d'apporter une plus-value aux travaux antérieurs, sans les dupliquer, la commission d'enquête a adopté une approche globale des politiques publiques pour y faire face dans une logique de contrôle et de l'évaluation de l'efficacité et l'efficience des dispositifs existants, en effectuant des visites sur place et en s'inspirant également d'exemples étrangers à l'occasion de déplacements de délégations de la commission à Bruxelles, ainsi qu'à Helsinki et Tallinn (cf. *liste des déplacements*).

Le rapporteur s'est en outre rendu à Taïwan dans un autre cadre que celui de la commission d'enquête, en rencontrant les autorités en charge de la lutte contre les influences étrangères, telles que la Vice-première ministre, le Ministre des affaires étrangères, et le Ministre en charge du numérique. Il a pu contribuer à ses travaux à ce titre¹.

Il en résulte dans une présentation du rapport de la commission en trois parties consacrées en premier lieu, à la France face aux influences étrangères malveillantes (première partie), puis aux outils et limites du dispositif actuel (deuxième partie) et, enfin, à la stratégie nationale préconisée par la commission (troisième partie) dont le volet programmatique à l'attention du Gouvernement s'articule en trois piliers et 47 recommandations nécessaires à leur mise en œuvre.

L'apport de la commission vise à dépasser le stade des constats pour passer à l'action. Les trois piliers de son approche se décomposent en trois objectifs :

- sortir de la naïveté par la résilience de la population ;
- sortir de la passivité en s'engageant dans la bataille des narratifs ;
- sortir de l'empirisme en se dotant d'une stratégie globale, nationale et interministérielle.

¹ *Déplacement de M. Rachid Temal, dans le cadre d'une délégation parlementaire composée de Mmes Else Joseph, sénatrice, Marie-Noëlle Battistel, députée, et M. Hadrien Ghomi, député, à l'occasion de l'investiture le 20 mai 2024 de M. Lai Ching-te, président de Taïwan.*

PREMIÈRE PARTIE : LA FRANCE CONFRONTÉE À UN DURCISSEMENT DES STRATÉGIES D'INFLUENCE

I. LA NOUVELLE DONNE GÉOPOLITIQUE ET TECHNOLOGIQUE : MENACES HYBRIDES ET BATAILLE DES PERCEPTIONS

A. UN ENVIRONNEMENT STRATÉGIQUE PLUS COMPLEXE, PLUS INCERTAIN ET PLUS DANGEREUX

1. Entre la désinhibition des puissances hostiles et la montée en puissance de l'hybridité sous le seuil de la guerre conventionnelle

Avant même la période contemporaine marquée par le retour de la guerre sur le sol européen, Thomas Gomart décrivait « **l'affolement du monde** »¹ - le titre d'un essai publié en janvier 2019 - comme la transformation inédite des rapports de force internationaux mettant en jeu l'ascension de la Chine, l'unilatéralisme américain, la fragmentation de l'Europe et le retour de la Russie sur la scène stratégique, sans compter de multiples tensions sur des sujets transversaux : l'énergie, le climat, le cyber, l'espace et la pression démographique et migratoire.

Déjà, la revue stratégique de 2017² s'inscrivait dans un « *contexte stratégique instable et imprévisible, marqué par une menace terroriste durablement élevée, la simultanéité des crises, l'affirmation militaire de puissances établies ou émergentes, l'affaiblissement des cadres multilatéraux et l'accélération des bouleversements technologiques* ». Tant l'actualisation stratégique de 2021 que la revue nationale stratégique de 2022 dressent le constat d'un monde chaotique où l'affrontement entre grands blocs, la désinhibition des puissances hostiles et l'irruption de guerres, qui ne disaient pas leur nom, deviennent le lot quotidien. Le **Général Lecointre**, ancien chef d'état-major des armées, a récemment résumé ainsi les dernières décennies de crises, notamment depuis le conflit en ex-Yougoslavie à la fin du XX^{ème} siècle : « *nous n'avons pas cessé d'être en guerre en réalité. Mais nous avons vécu dans une bulle* ».

Ces grandes tendances se sont accélérées : compétition entre grandes puissances, généralisation des stratégies hybrides, enhardissement des puissances régionales, effets de rupture liés aux nouvelles technologies, notamment numériques et informationnelles (cf. illustration infra).

¹ Thomas Gomart, *L'affolement du monde. 10 enjeux géopolitiques*, Taillandier, 2019.

² Secrétariat général de la défense et de la sécurité nationale, [Revue stratégique de défense et de sécurité nationale 2017](#).

Illustrations relatives à la diversité des menaces hybrides couvrant aussi bien les champs du cyber et de l'informationnel que de la contrainte ou de la coercition armée



Source : SGDSN

La montée en puissance capacitaire dans le domaine de la guerre conventionnelle des pays dits « compétiteurs », à l'exemple de l'effort de la Chine dans la construction navale (construction du tonnage de l'équivalent de la flotte française tous les 4 ans) ou de l'Iran dans le domaine des missiles balistiques et des drones, se double dorénavant de la démonstration sur le terrain de ces nouveaux moyens. La multiplication des tirs de missiles et de drones par l'Iran ou d'États et de milices affiliées, par la Corée du Nord, ou des cas de confrontations entre la Chine et les États riverains, notamment les Philippines, de la mer de Chine méridionale témoigne d'une désinhibition de l'emploi de toute la panoplie des menaces dites hybrides précédemment évoquées en introduction.

Le fait nouveau réside dans le développement sans précédent de ces menaces, particulièrement dans le domaine informationnel. Ainsi que le soulignait le professeur David Colon, entendu par la commission, « à l'équilibre de la guerre froide a succédé le déséquilibre de la guerre de l'information »¹.

Ce déséquilibre est illustré par les chiffres de la cybercensure en Chine, rapportés par Reporter sans frontières (RSF) : le pays a dépensé environ 5,5 milliards d'euros en matière de cybercensure² en 2020 et au moins 2 millions de personnes travaillaient déjà en 2013 pour le contrôle des opinions exprimées sur les réseaux chinois. Comme l'a souligné le capitaine de vaisseau Yann Briand, sous-directeur des affaires internationales du secrétariat général de la défense et de la sécurité nationale (SGDSN), les défis

¹ [Audition](#) du 29 février 2024.

² Source: The Jamestown foundation “Buying Silence: The Price of Internet Censorship in China” (janvier 2021)

qui se posent aux démocraties sont colossaux car si pour le moment, la menace principale en matière cyber et informationnelle est russe, on pourrait considérer que « *si la Russie est une vague, la Chine est potentiellement un tsunami* »¹.

2. Montée en puissance des menaces hybrides et définition de l'influence comme 6^{ème} fonction stratégique des armées

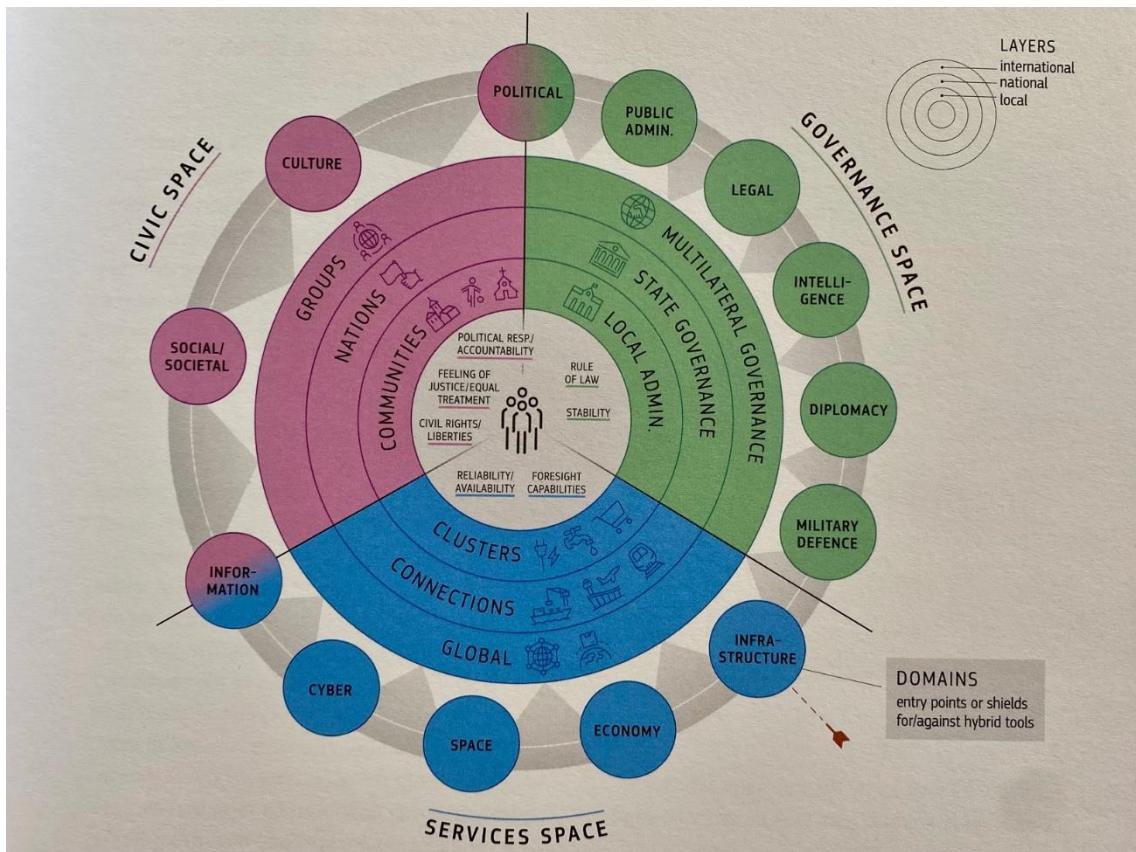
La prise en compte de l'enjeu des menaces hybrides est relativement récente puisque le Centre d'excellence sur les menaces hybrides de l'OTAN et de l'Union européenne n'a été créé qu'en 2017 à l'initiative notamment de la Finlande, dont la population, avant même son adhésion à l'organisation transatlantique, se révèle particulièrement sensible aux risques multiformes que son voisin russe fait peser sur son territoire et ses infrastructures.

L'une des caractéristiques propres aux pays nordiques est l'adoption d'un modèle d'analyse des menaces matérialisé comme un « écosystème global de résilience »². Ainsi, le Centre d'excellence d'Helsinki a développé une grille d'analyse de l'ensemble des domaines, civiles ou militaires, publics ou privés, économiques ou politique, pouvant porter une attaque sur un État, dans l'ensemble de ses composantes (cf. schéma ci-après).

¹ [Audition](#) du 27 février 2024.

² Modèle «CORE» (Comprehensive resilience ecosystem) – Rapport EUR 31104 EN (mars 2023)

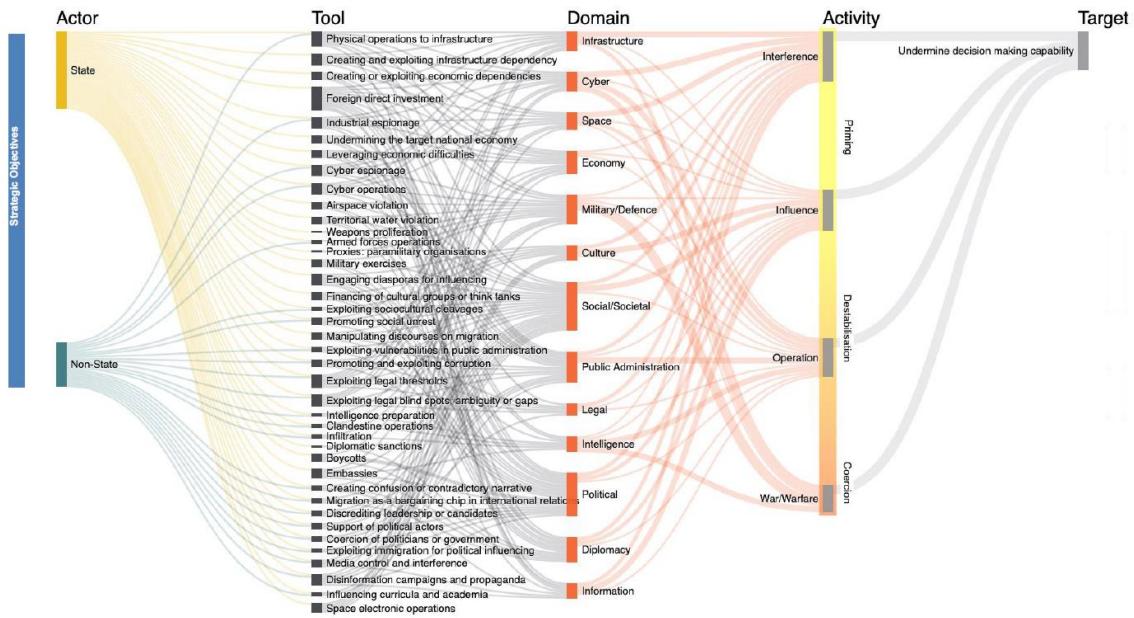
Modèle d'analyse de l'écosystème global de résilience face aux menaces hybrides



Source : Centre d'excellence d'Helsinki

Cette approche globale se caractérise par un champ extrêmement large des stratégies et objectifs d'attaque à analyser. Ainsi que l'illustre le schéma ci-dessous, outre la variété des acteurs (étatiques ou non-étatiques), les outils (*tool*), domaines d'action et activités s'étendent des ingérences (*interference*) à la guerre proprement dite (*war*) en passant par une zone grise mêlant influences et opérations de déstabilisation, sans frontières nettes et précises entre elles, qui toutes convergent vers une seule et même cible (*target*).

Représentation des voies et moyens des attaques hybrides



Source : Centre d'excellence d'Helsinki

Transposé en France dans le cadre d'un document non public de référence interministériel sur les stratégies hybrides élaboré en mars 2021 par le secrétariat général de la défense et de la sécurité nationale (SGDSN) qui a la charge de coordonner cette matière, une stratégie hybride s'entend comme « *le recours par un acteur étatique ou non à une combinaison intégrée et volontairement ambiguë de modes d'actions militaires et non militaires, directs et indirects, légaux ou illégaux, difficilement attribuables. Jouant avec les seuils estimés de riposte et de conflit armé, cette combinaison est conçue pour contraindre et affaiblir l'adversaire, voire créer chez lui un effet de sidération* ».

En novembre 2022, dans le cadre de l'annonce faite par le Président de la République de mettre fin à l'opération Barkhane, au cours de laquelle les forces françaises ont fait l'objet de campagnes informationnelles organisées par la Russie ou des entités et individus pro-russes, il était également annoncé que l'influence serait érigée par la Revue nationale stratégique 2022 (RNS 2022) au rang de 6^{ème} fonction stratégique, en plus des cinq fonctions stratégiques traditionnellement dévolues aux armées : protection, dissuasion, intervention, prévention, connaissance et anticipation (renseignement).

Le constat exprimé par le Président de la République faisait explicitement référence aux opérations d'influences étrangères dirigées contre les intérêts français : « *on a vu, comme en Afrique, souvent à l'instigation d'acteurs extérieurs, des récits malveillants s'implanter, être démultipliés par des jeux de miroir par des bots, des trolls et tout un bestiaire digital mis à contribution dans une manœuvre très bien intégrée, il faut bien le dire, par plusieurs de nos rivaux pour contester notre sécurité et notre rayonnement. Et propager, outre de faux récits, un*

appétit de violence, manipuler les populations civiles et, en quelque sorte, accroître encore l'hybridité des conflits »¹.

Ce constat se doublait déjà d'une **volonté de sortir de la passivité ou d'une posture purement défensive pour assumer une communication plus active** sur la position de la France : « *il nous revient aussi de penser la promotion, sans orgueil mais sans inhibition malvenue, de notre cause* » car une « *attitude qui serait seulement réactive, voire défensive, pourrait passer pour une forme de passivité. Ce ne sera pas la nôtre* ».

B. PLATEFORMES, INTELLIGENCE ARTIFICIELLE... : DE NOUVEAUX CANAUX DE PERCEPTION DE L'INFORMATION

Quand Jean-Yves Le Drian, alors ministre de l'Europe et des affaires étrangères déclarait « *il n'y a plus de soft power, il n'y a que du hard power* »² à l'occasion de la présentation de la **feuille de route de l'influence de la diplomatie française**, il était fait référence au changement d'attitude tant de la Russie que de la Chine, mais aussi de nouveaux compétiteurs régionaux tels que la Turquie, vers une communication officielle délibérément agressive, voire mensongère (cf. *infra*) qui ne relève dès lors plus de la traditionnelle influence légitime (*soft power*) mais glisse vers ce que la définition du SGDSN des menaces hybrides classe dans **l'influence malveillante**.

1. La nouvelle donne technique et numérique opère comme un effet multiplicateur des manipulations de l'information

La conjonction de la nouvelle donne géopolitique avec de nouveaux canaux de perception de l'information, mettant en œuvre des technologies algorithmiques et l'intelligence artificielle, a pu être présentée au cours des tables rondes technologiques comme un multiplicateur des manipulations et des effets de bulle informationnelle.

Deux constats ont pu être établis :

- celui de la méfiance envers les « grands médias » sur les sujets d'actualité (57 % des Français interrogés jugent qu'il faut « *se méfier de ce que disent les médias sur les grands sujets d'actualité* »)³ ;

- de deuxièmement, selon le même sondage, 24 % des moins de 35 ans s'informent via des influenceurs. D'autre part, il faut relever que les jeunes électeurs européens de 18 à 25 ans placent les réseaux sociaux TikTok (29 %)

¹ [Déclaration du président de la République Emmanuel Macron sur la Revue nationale stratégique et la programmation militaire de la France](#), à Toulon le 9 novembre 2022

² [Discours du ministre de l'Europe et des affaires étrangères Jean-Yves Le Drian](#) à la Conférence des ambassadeurs et des ambassadrices (août 2019)

³ Source : baromètre annuel *La Croix-Kantar sur la confiance des Français dans les médias* publiés en novembre 2023

et Instagram (27 %) en deuxième et troisième positions derrière la télévision (47 %)¹.

Les quatre auditions organisées avec les plateformes Meta, X (ex-Twitter), Google et TikTok ont permis de mieux comprendre les mécanismes de modération des contenus mais aussi le rôle central des algorithmes dans l'accès des utilisateurs à l'information et dans le modèle économique de ces réseaux.

2. Guerre informationnelle, bataille des perceptions

Dans la présentation faite à la commission par **Guy-Philippe Goldstein** sur **la guerre cognitive et la polarisation de la guerre froide 2.0**, il explique que les plateformes de réseaux sociaux tendent à favoriser la diffusion de messages « *surprenants et négatifs* » ainsi que l'instabilité émotionnelle et l'extrémisme².

Dans une analyse des cascades de rumeurs sur Twitter de 2006 à 2017 (126 000 histoires « tweetées » par 3 millions de personnes plus de 4,5 millions de fois), **les nouvelles fausses et surprenantes ont 70 % plus de chances d'être retweetées** que des informations fiables sur des événements réels. Les fausses nouvelles atteignent une « « profondeur de cascade (chaînes de retweets ininterrompues) de 10 à environ 20 fois plus rapidement que des faits réels.

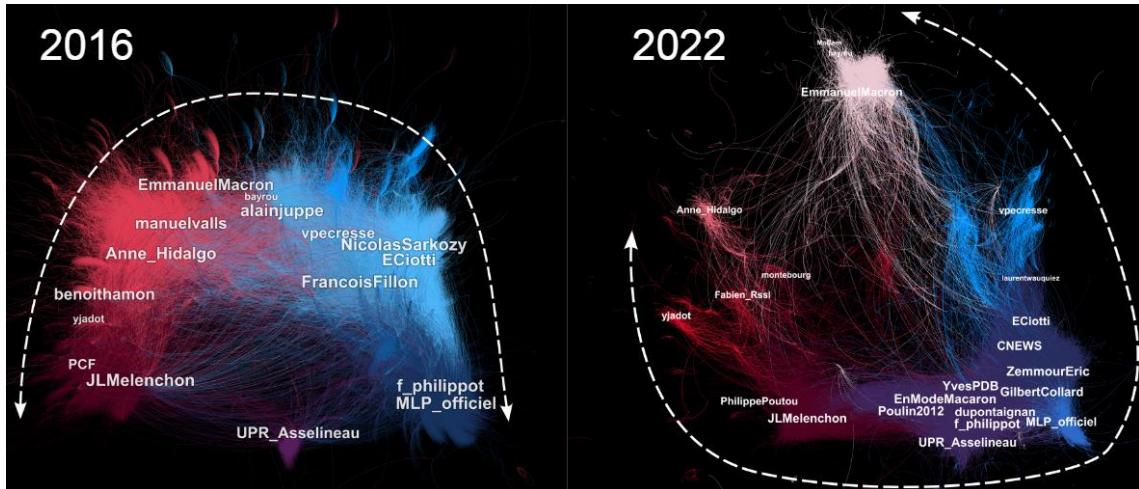
Cette bataille des perceptions a également été modélisée par **David Chavalarias**, directeur de recherche au CNRS auditionné par la commission d'enquête³, au moyen d'une **étude sur l'évolution de la « twittersphère » politique de 2016 à 2022**. Les deux représentations ci-dessous présentent sous forme de filaments des échanges entre comptes Twitter.

¹ Source : sondage Ifop pour l'Anacej et Les Jeunes Européens, « [Les jeunes et les élections européennes de 2024](#) », avril 2024.

² [Audition](#) du 20 juin 2024.

³ [Audition](#) du 4 juin 2024.

Modélisation de l'évolution de la twittosphère politique entre 2016 et 2022



Source : David Chavalarias

Les filaments « matérialisent la circulation d'information au sein du réseau via l'action de partage (retweet). Les échanges entre plusieurs dizaines de milliers de comptes Twitter sont représentés sur chaque figure, les labels correspondants aux comptes des personnalités politiques les plus représentatives de leur région. En 2016, les partis traditionnels PS et LR sont au cœur de la circulation d'information. Six ans plus tard, les partis d'extrême-droite sont au cœur de la circulation d'information tandis que les communautés PS et LR se sont effilochées. La communauté anti-système qui a émergé autour de Florian Philippot (en violet) fait une passerelle entre LFI et le bloc d'extrême droite »¹.

II. DES COMPÉTITEURS ENGAGÉS DANS UNE GUERRE D'INFLUENCE CONTRE LA FRANCE : CARTOGRAPHIE DE LA MENACE

Le présent rapport, qui vise à passer en revue et renforcer nos outils de lutte face aux opérations d'influence étrangères malveillantes d'où que celles-ci proviennent, n'a pas vocation à se concentrer sur la menace émanant d'un ou plusieurs acteurs particuliers, ni à formuler de préconisation sur la politique diplomatique à conduire vis-à-vis de tel ou tel État.

Pour autant, il a semblé important à la commission d'enquête de présenter les principaux compétiteurs, identifiés au cours des différentes auditions conduites, menant des opérations d'influence malveillantes ciblant la France.

¹ David Chavalarias, [Minuit moins dix à l'horloge de Poutine : : Analyse de réseaux des ingérences étrangères dans les élections législatives de 2024](#), juillet 2024

A. À L'INSTAR DES AUTRES PAYS OCCIDENTAUX, LA FRANCE EST PRISE POUR CIBLE PAR LES GRANDES PUISSANCES RÉVISIONNISTES QUE SONT LA RUSSIE ET LA CHINE

Les auditions conduites par la commission d'enquête ont largement permis de conforter le constat posé par la Revue nationale stratégique de 2022¹, qui pointe les « *ambitions révisionnistes exacerbées* » de la Fédération de Russie et de la République populaire de Chine, se caractérisant par des « *pratiques de contestation et de contournement de l'ordre international fondé sur le multilatéralisme et la règle de droit (...) édifié depuis la fin de la guerre froide* », participant d'une « *convergence stratégique croissante* » entre ces deux pays. Un tel retour des empires contrariés sur la scène géostratégique est la source de bouleversements majeurs.

La même Revue nationale stratégique fait ainsi état de la « *stratégie de remise en cause de la sécurité européenne, dont la guerre engagée contre l'Ukraine le 24 février 2022 représente la manifestation la plus ouverte et la plus brutale* », conduite par la Russie, qui conçoit sa puissance comme « *une opposition à (...) l'Occident collectif* ».

S'agissant de la Chine, elle relève que, « *au-delà de sa pérennisation au pouvoir, l'objectif du parti communiste chinois (PCC) et de l'armée populaire de libération (APL) reste de supplanter les États-Unis comme première puissance mondiale. Considérant la puissance américaine et le modèle occidental en déclin, le régime chinois estime que le leadership occidental sur l'ordre international est fragilisé et qu'il peut l'affaiblir encore davantage en mettant à profit son influence nouvelle* ».

C'est dans le cadre de cette confrontation stratégique que ces deux États sont amenés, tout en restant sous le seuil du conflit armé, à mener des opérations d'influence malveillantes contre les pays occidentaux, au premier rang desquels les États-Unis, mais également la France, qui constitue une cible de choix pour ces deux pays. La rivalité entre la Chine et les États-Unis s'exprime d'ailleurs avec une intensité particulière dans l'Indopacifique, où la France est la seule nation de l'Union européenne à y être présente.

1. La Russie, compétiteur le plus agressif

a) Une guerre d'influence contre l'Occident

Dans le domaine de la guerre d'influence, la Russie est indéniablement le compétiteur le plus agressif.

La guerre hybride, en particulier dans sa dimension informationnelle, est profondément inscrite dans la **tradition stratégique russe**. Comme le relève l'historien David Colon : « *la désinformation s'inscrit en Russie dans une tradition vieille de plusieurs siècles. L'État russe, en effet, depuis Catherine II et Grigori Potemkine, a fait de la manipulation des perceptions une politique nationale*

¹ Secrétariat général de la défense et de la sécurité nationale, [Revue nationale stratégique 2022](#).

tandis que l'armée russe a poussé à la perfection l'art de la tromperie militaire (maskirovska) »¹.

Cette tradition a su s'adapter à la nouvelle donne technique liée à l'avènement du numérique : « aux notions occidentales de "cybersécurité" et de "cyberdéfense" qui mettent en avant les contenus (infrastructures, terminaux), la doctrine militaire russe préfère depuis longtemps celles de "sécurité informationnelle" et de "défense informationnelle", qui associent les contenus et les contenus pour qualifier un terrain de conflictualité virtuel, "l'espace informationnel". (...) Depuis les années 1970, la doctrine militaire russe s'appuie sur la notion de "contrôle réflexif" qui consiste à influencer la perception qu'ont les adversaires de leur environnement en agissant sur les "sphère informationnelle" (...), soit pour encourager l'adversaire à agir dans un sens donné, soit pour créer la confusion et paralyser sa décision »².

La posture russe à l'égard de ce qu'elle désigne comme « l'Occident » se fait plus agressive depuis la fin des années 2000. Toujours selon David Colon, dès 2007-2008, à mesure que la crise économique frappe la Russie, la propagande, relayée par des agences de relations publiques occidentales, « se concentre sur une vision noire du monde occidental, présenté comme décadent et corrompu »³.

La campagne de réélection de Vladimir Poutine en 2012, au cours de laquelle celui-ci a accusé les puissances occidentales de tentatives de manipulation de l'opinion russe pour le faire battre, et le déclenchement d'une « guerre hybride » en Ukraine à compter de 2013, ont marqué un nouveau tournant. Dès lors, « la stratégie russe du chaos est appliquée à grande échelle pour affaiblir l'Europe en remettant en cause tant son unité que son soft power politique et culturel (...). Pour ce faire, la propagande russe donne une caisse de résonnance à toutes les forces centrifuges, à toutes les voix critiques ainsi que le plus grand retentissement possible aux tensions sociales et aux attentats terroristes »⁴. Les ingérences russes documentées dans la campagne référendaire britannique sur la sortie de l'Union européenne pour favoriser le camp du « Brexit » et dans les élections présidentielles états-uniennes de 2016 pour favoriser Donald Trump sont les illustrations les plus éclatantes de son action.

Dans cette guerre livrée à l'Occident, « l'influence est un substitut à une puissance que le Kremlin n'a plus. Ce dernier investit d'autant plus dans les opérations d'influence qu'il n'est plus en mesure de peser sur les destinés militaires ou celles économiques du monde comme il a pu rêver de le faire, par le passé »⁵.

Cette stratégie, soutenue par l'administration présidentielle russe, est supervisée et déclinée par les services de renseignement, puis exécutée par

¹ David Colon, *La guerre de l'information. Les États à la conquête de nos esprits*, Taillandier, septembre 2023, pp. 236-237.

² David Colon, op. cit., p. 80.

³ David Colon, op. cit., p. 89.

⁴ David Colon, op. cit., p. 178.

⁵ [Audition](#) de David Colon du 29 février 2024

d'autres relais, dans le but de gagner l'adhésion tant de la diaspora russophone que des milieux russophiles dans les pays occidentaux.

Elle s'appuie sur plusieurs acteurs, présentés par Maxime Audinet, spécialiste de la politique d'influence russe auditionné par la commission d'enquête¹, témoignant du fait que la Russie y consacre des moyens sans commune mesure avec l'ensemble des autres acteurs.

En premier lieu, des acteurs étatiques :

- les services de renseignement, qui mènent des opérations d'ingérence ;

- les acteurs de la diplomatie numérique, soit la communication officielle des ambassades, du ministère des affaires étrangères et du ministère de la défense russes, qui, relève d'une politique d'influence malveillante non dissimulée. L'activisme diplomatique de l'ambassadeur en France, Alexander Makogonov, est notamment cité.

- les médias d'État transnationaux, tels que *Russia Today* et *Sputnik* ;

En second lieu, on trouve des acteurs non officiels qui n'appartiennent pas à l'État mais à une frange désinstitutionnalisée de l'État russe, tels que :

- des « entrepreneurs d'influence », dont Evguéni Progojine, le fondateur récemment décédé du groupe Wagner, mué en « *African Initiative* » sur le continent africain, et des « usines à *trolls*² » du projet Lathka, constitue l'incarnation ;

- des « contractuels de l'influence », soit des « *prestataires d'influence ou de désinformation* », voire de véritables « *technologies politiques* », sous-traitées par l'administration présidentielle. Maxime Audinet prend l'exemple du « Centre S », qui « *constitue un acteur déterminant des ingérences informationnelles de la Russie dans nos démocraties* ».

Jusqu'à l'invasion à grande échelle de l'Ukraine le 24 février 2022, la Russie menait dans le même temps une politique d'influence agressive et une politique de *soft power* plus traditionnels, comme en témoigne l'organisation des jeux Olympiques de Sotchi en 2014 et de la coupe du monde de football en 2018. Depuis lors, la guerre informationnelle lancée est totale, bien que s'inscrivant dans le prolongement direct de la période précédente.

¹ Audition du 7 mars 2024.

² Les « usine à *trolls* » pro-russes sont des acteurs qui s'emploient à diffuser massivement des contenus favorables au narratifs pro-russes sur les réseaux sociaux. Les *trolls* peuvent être définis comme des messages postés sur les réseaux sociaux « internautes qui provoquent délibérément leurs adversaires dans le but de les offenser, de les ridiculiser et de les contraindre au silence ». Les messages sont souvent générés par des bots, soit un « agent logiciel automatique ou semi-automatique qui interagit avec des serveurs informatiques pour générer des connexions, créer des faux-comptes, amplifier artificiellement des contenus par des likes et des partages, et diffuser des contenus » (David Colon, op. cit., pp. 455-457).

b) La France, cible privilégiée de la guerre d'influence russe

La France est spécifiquement prise pour cible par la Russie à deux titres au moins.

En premier lieu, en tant que puissance occidentale membre de l'Otan, et participant activement au soutien aux forces armées ukrainiennes, elle est assimilée à « l'Occident collectif » honni.

C'est notamment à compter de 2018 que la Russie, parvenue, selon David Colon, à constituer en France un « très vaste réseau d'experts, de militaires, d'anciens espions, de journalistes, de femmes et d'hommes politiques qui, par idéologie, stratégie politique, croyance religieuse, intérêt personnel ou appât du gain, relaient volontiers dans les médias les narratifs russes ».

Lors de son audition, Nicolas Tenzer détaille notamment les principales idées présentées dans le cadre des narratifs poussés dans les médias et sur les réseaux sociaux par les acteurs pro-russes concernant la guerre en Ukraine : « la faute est partagée » entre russes et Ukrainiens ; « l'Otan est une menace pour la Russie » ; « de toute manière, la guerre est perdue pour l'Ukraine » ; « il ne faut pas humilier la Russie » ; « on ne peut pas défaire une puissance nucléaire »¹.

En second lieu, la France est prise pour cible au titre de sa présence sur le continent africain, où la Russie entend déployer son influence de façon accrue, notamment depuis 2018-2019 et l'organisation du sommet russo-africain de Sotchi des 23 et 24 octobre 2019.

La Russie livre depuis une guerre informationnelle de grande ampleur contre la France en particulier dans le Sahel, ciblant ses opérations militaires. Elle repose notamment sur l'action du groupe Wagner, n'hésitant pas à y dénoncer un présumé « néo-colonialisme » pour exploiter le sentiment anti-français d'une partie des populations.

2. La Chine, une menace croissante

La Chine est un autre acteur important de l'ingérence et de l'influence, mais selon des modalités différentes de la Russie, beaucoup moins agressives : il s'agit pour elle non pas de s'en prendre à notre modèle, comme le fait la Russie, mais de promouvoir le sien.

La stratégie chinoise à l'égard de l'Occident a, cependant, connu une mutation importante et progressive depuis la fin des années 2000. Pour reprendre l'expression de Jean-Baptiste Jeangène Vilmer et Paul Charon, chercheurs à l'Institut de recherche académique de l'École militaire (Irsem), la Chine connaît en effet un « *moment machiavélien* » - en référence à la célèbre formule de Machiavel qui écrivait dans *Le Prince* (1532) qu'« *il est plus sûr d'être*

¹ [Audition](#) du 29 février 2024.

craint que d'être aimé » - correspondant à une forme de « *russianisation* » de sa politique étrangère¹.

Comme l'explique Paul Charon lors de son audition par la commission d'enquête² : la Chine est même en capacité de « *mener des opérations plus larges que la Russie, car elle dispose de plus de moyens financiers, mais aussi de ressources humaines importantes* ».

La Chine est ainsi « *[passée] d'une propagande positive (...), visant à la présenter comme un acteur bienveillant, proposant des relations gagnant-gagnant, cherchant une émergence pacifique sur la scène internationale, à un autre type de contenu. Si la propagande positive n'a pas disparu, elle est concurrencée par un contenu devenu agressif et dépréciatif, en particulier envers les États-Unis, qui peut aussi cibler des valeurs.* »

Outre la promotion de son modèle politique et la dépréciation de la démocratie, qui s'inscrivent dans l'objectif d'assurer la pérennité de son régime, la Chine poursuit, au travers de sa politique d'influence, des objectifs d'ordre géopolitique. Comme l'explique Paul Charon : « *les Chinois ont intérêt à diviser l'Europe. La Chine est plus forte et plus à l'aise dans les relations bilatérales. Le leadership chinois est bien conscient qu'il obtiendrait moins s'il avait en face de lui un interlocuteur unique en Europe. Il est également dans l'intérêt de la Chine de tenter d'éloigner l'Europe des États-Unis. Le traitement de la guerre en Ukraine par les médias chinois en témoigne : la guerre est présentée comme voulue et mise en œuvre par les États-Unis, au détriment de l'intérêt des Européens. (...) De la même manière, à l'échelle internationale, la Chine essaie d'éloigner ce qu'elle appelle le "Sud global", de l'Europe* ».

S'agissant de l'organisation du dispositif chinois, Paul Charon a regretté « *notre insuffisante connaissance des acteurs et des objectifs réels visés, au-delà des objectifs stratégiques, par l'appareil de la propagande chinoise* », qui procède « *d'un manque de moyens* ».

Pour, Valérie Niquet, spécialiste de la Chine à la Fondation pour la recherche stratégique (FRS) les organes de propagande extérieure dépendent de la commission des affaires extérieures du Parti communiste chinois, avec à sa tête le président Xi Jinping. Ces organes sont pilotés par le Groupe dirigeant pour le travail de la propagande idéologique, « *qui contrôle et organise le travail dans toutes ses dimensions* » en s'appuyant notamment sur :

- le ministère des affaires étrangères et le réseau d'ambassades ;
- des médias contrôlés par le PCC, tels que l'agence de presse Xinshua.

Outre les acteurs étatiques, à l'instar de la Russie, la Chine s'appuie sur la mobilisation d'organisations formellement extérieures à l'État ou au

¹ Paul Charon et Jean-Baptiste Jeangène Vilmer, « *Les Opérations d'influence chinoises. Un moment machiavélien* », rapport de l'Institut de recherche stratégique de l'École militaire (Irsem), Paris, ministère des armées, septembre 2021 – rapport téléchargeable [ici](#).

² [Audition](#) du 6 juin 2024.

Parti. Il s'agit de la stratégie du « front uni ». Ainsi, « *de grandes entreprises comme Alibaba ou Huawei pourraient être mobilisées au service de l'image de la Chine* ». Au plan de la guerre informationnelle, l'armée populaire de libération (APL), s'appuie également sur des « *ingénieurs civils et des hackers "patriotiques" (...) [qui] fournissent les armées de trolls et les opérations de pénétration et de submersion des réseaux ennemis* »¹.

Elle s'appuie également sur les **diasporas**, bien que celles-ci soulèvent pour le régime « *une question ambiguë* », comme l'explique Paul Charon lors de son audition. En effet, il s'agit d'une « *population qui « maîtrise parfaitement la langue et la culture chinoises et qui, parce qu'elle ne cesse de faire des allers-retours entre les pays d'accueil et la Chine, est susceptible d'importer des valeurs libérales auxquelles elle a été exposée* ». Elle constitue donc une « *menace* », de telle sorte que « *le premier objectif du PCC est de la contrôler partout dans le monde* ». Cela passe notamment par « *la maîtrise des médias en langue chinoise à l'étranger* » mais aussi par « *des actions physiques. Cette menace a été qualifiée d'« infiltration culturelle » en 2015* dans le cadre des débats autour de la loi sur la sécurité nationale.

Le réseau social TikTok constitue également une menace, bien mise en évidence par les travaux récents de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence². Pour Paul Charon, s'il ne s'agit pas « *du principal vecteur de l'influence de la Chine* », la plateforme, qui est à l'évidence « *sous la coupe de la Chine* », en ce qu'elle peut capter les données des utilisateurs peuvent être utiles, « *ne serait-ce que pour nourrir les intelligences artificielles chinoises* » qui pourraient, demain, être mises au service de nouveaux outils d'influence.

Pour autant, il convient de relever qu'à la différence de la Russie, la Chine ne fait pas de la France une cible majeure et qu'« *il n'a pas véritablement de spécificité dans la manière dont les Chinois visent la France* », par comparaison aux autres pays occidentaux. Certes, elle représente un enjeu important dans la mesure où la diaspora chinoise représente plusieurs centaines de milliers de personnes. Par ailleurs, « *la France est également accusée par les Chinois, comme elle l'est par les acteurs pro-russes, de mener des activités liées ou assimilées à du néocolonialisme, notamment en Afrique* ».

¹ Valérie Niquet, « *La Chine : une modernisation des pratiques de guerre de l'information* » in Céline Marangé et Maud Quessard (dir.), *Les guerres de l'information à l'ère numérique*, Presses universitaires de France, janvier 2021, pp. 148-157.

² [Rapport n° 831 \(2022-2023\)](#) fait par Claude Malhuret au nom de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence, déposé le 4 juillet 2023.

B. DES MENACES ÉMERGENTES « TOUS AZIMUTS »

Outre les deux grands compétiteurs stratégiques que sont la Russie et la Chine, la commission d'enquête a identifié une importante variété d'acteurs étrangers, d'origine étatiques ou non étatiques, menant des opérations d'influence malveillantes ciblant la France, avec des finalités diverses.

1. Des compétiteurs étatiques émergents : Azerbaïdjan, Turquie, Iran

Certains compétiteurs émergents poursuivent des intérêts géopolitiques les conduisant à mener de telles opérations en direction de la France.

En particulier, suite aux prises de position françaises envers l'Arménie, nous nous sommes découverts un nouveau compétiteur avec l'Azerbaïdjan, qui a mené des opérations d'ingérence d'une particulière hostilité à l'égard de la France dans la période récente (voir *infra, IV*), dénoncées notamment par le ministre de l'intérieur et des Outre-mer, Gérald Darmanin¹, et le ministre de l'Europe et des affaires étrangères, Stéphane Séjourné², lors de leurs auditions par la commission d'enquête. Ce dernier allant même jusqu'à évoquer une « *crise inédite* » des relations entre la France et l'Azerbaïdjan.

Inspiré et encouragé par la Russie, ce pays s'appuie sur des structures non-étatiques pour mener ses opérations d'influence, tels que le **Baku Initiative Group (BIG)**. Selon une logique de « *puissance tranchante* » (voir *Introduction*), ces opérations poursuivent essentiellement un objectif de déstabilisation de la société française par le biais de la recherche d'une amplification des tensions sociales. Son action se déploie dans l'hexagone mais également dans les Outre-mer, et en particulier en Polynésie française et en Nouvelle-Calédonie, avec la volonté d'instrumentaliser les récentes émeutes. Reprenant une méthode éprouvée par la Russie, les acteurs pro-Azerbaïdjan y dénoncent à leur tour un présumé « colonialisme français ».

La **Turquie**, dont les ressortissants composent la troisième communauté étrangère présente sur notre territoire national, agit selon une logique différente : il s'agit de préserver son identité contre toute forme d'acculturation. Elle possède en France une forte représentation diplomatique, qui sert à appuyer l'activité de ses services de renseignement. D'autres structures sont par ailleurs à la manœuvre pour collecter des informations et développer une stratégie d'influence.

¹ [Audition](#) du 28 mai 2024

² [Audition](#) du 18 juin 2024.

Ce pays dispose de quatre principaux leviers d'action :

- le contrôle communautaire, qui permet de surveiller la diaspora, de s'assurer de son soutien au gouvernement turc et de juguler l'opposition ;

- l'encadrement de la pratique religieuse de la communauté (voir *infra*) ;

- l'ingérence politique ;

- l'influence informationnelle, notamment dans les années récentes, notamment au moyen d'une diplomatie publique agressive. Celle-ci porte essentiellement sur la dénonciation de notre modèle de laïcité, qui témoignerait d'une prévue « *islamophobie* » française. Des opérations de communication d'ampleur, impulsées notamment par le président Recep Tayyip Erdogan, ont été menées contre la France dans le sillage de l'assassinat de Samuel Paty en octobre 2020 puis dans le contexte de l'examen du projet de loi confortant le respect des principes de la République.

Depuis 2022, le média international turc TRT s'est doté d'une chaîne en français pour faire valoir « un narratif alternatif » à destination notamment de l'Afrique.

Le cas de l'**Iran** a également été cité à plusieurs dans le cadre des auditions menées par la commission d'enquête, quoique dans une moindre mesure. Les services iraniens agissent sur deux axes principaux : le contrôle de leur opposition, et une pression diplomatique forte pour que la France modère les positions qu'elle peut prendre envers ce pays. Sa diplomatie publique, contrôlée par le Corps des Gardiens de la révolution, constitue un élément clé d'une stratégie asymétrique menée en direction des adversaires du régime. **Comme la Russie, elle s'appuie notamment sur son audiovisuel extérieur, l'IRIB**¹. En particulier, la chaîne satellitaire Press-TV, diffusée en anglais et en français, cible un public occidental pour y défendre les narratifs pro-iraniens². Elle s'appuie également sur la communication officielle des autorités sur les réseaux sociaux, comme en témoigne le récent soutien public exprimé sur X (ex-Twitter) par l'Ayatollah Khamenei aux mouvements étudiants propalestiniens dans les pays occidentaux, prenant en exemple une photo de manifestations à Sciences Po Paris.

¹ Islamic Republic of Iran Broadcasting.

² Pierre Pahlavi, « L'Iran : stratégie asymétrique et diplomatie de masse » in Céline Marangé et Maud Quessard (dir.), op. cit., pp. 181-200.

2. Les influences d'inspiration islamiste : une menace endogène ou d'origine étrangère ?

La commission d'enquête s'est également penchée sur la question des influences d'inspiration islamiste¹, en particulier lorsque celles-ci prônent un séparatisme susceptible de porter atteinte à la cohésion nationale, voire de conduire au terrorisme.

La question du terrorisme déborde le champ d'investigation de la commission d'enquête, les attentats commandités par les grandes organisations terroristes internationales constituant des opérations armées qui, bien qu'ayant pour objectif essentiel de produire un effet psychologique sur la population, ne sauraient être considérées comme de l'influence *stricto sensu*. Pour autant, la problématique du terrorisme n'est pas étrangère à celle de la radicalisation et du séparatisme.

Les influences d'inspiration islamiste diffusées dans l'espace informationnel français constituent ainsi, à ce titre, une préoccupation majeure. Eu égard au champ de compétence de la commission d'enquête, il s'est avéré nécessaire de vérifier dans quelle mesure ces influences peuvent être considérées comme étant d'origine étrangère.

Indéniablement, l'islamisme trouve son origine dans des mouvances extra-européennes. Les quatre formes d'islamisme identifiées par Bernard Rougier, auditionné par le rapporteur, en témoignent : l'idéologie des **Frères musulmans** (ou frérisme), qui est d'origine égyptienne, le Tabligh qui provient du sous-continent indien, ainsi que le salafisme et le djihadisme ont tous été forgées dans le monde musulman. Pour autant, comme ce dernier le précise par ailleurs, « *les principaux réseaux religieux en France peuvent s'analyser comme des formes d'acculturation hexagonale de l'islamisme moyen-oriental* »².

Le constat selon lequel **le frérisme en Europe, en particulier, serait aujourd'hui un phénomène principalement endogène** est conforté par Olivier Roy, autre spécialiste de la question auditionné par le rapporteur, ainsi que par deux hauts fonctionnaires, l'ambassadeur François Gouyette et le préfet Pascal Courtade, à qui le ministre de l'intérieur et des Outre-mer et le ministre de l'Europe des affaires étrangères ont confié en mai 2024 une mission sur l'islamisme politique et la mouvance des Frères musulmans. Dans son ouvrage consacré au frérisme, Florence Bergeaud-Blacker souligne l'ancrage

¹ *L'islamisme peut être défini comme « le refus assumé de distinguer l'islam comme religion, l'islam comme culture et l'islam comme idéologie, ainsi que par le souci de soumettre l'espace social, voire l'espace politique, à un régime spécifique de règles religieuses promues et interprétées par des groupes spécialisés ».* Source : Bernard Rougier (dir.), *Les territoires conquis de l'islamisme*, Presses universitaires de France, janvier 2020, p. 19.

² Bernard Rougier (dir.), *Les territoires conquis de l'islamisme*, Presses universitaires de France, janvier 2020, pp. 19.

ancien et même « *l'institutionnalisation* » des Frères en Europe, qui remonte aux années 1960¹.

Leur acculturation aux sociétés européennes a une incidence sur leur stratégie. Comme l'a souligné Olivier Roy lors de son audition, celle-ci repose sur une défense de « droits » des musulmans en tant que « minorité » inspirés de thèses « multiculturalistes ». Dans ce cadre, la thématique du droit au port du voile comme « levier d'affirmation identitaire » est particulièrement mis en avant.

Cela étant, **des influences étrangères peuvent continuer de venir soutenir cette mouvance, même si leur caractérisation est délicate**. Comme le résume Étienne Apaire, secrétaire général du comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR) lors de son audition par la commission d'enquête : « *nous avons des nationaux sous influence étrangère ou relayant des influences étrangères et des étrangers ne relevant d'aucun État précis qui essaient de nous influencer en promouvant des valeurs, des modes d'organisation ou des croyances contraires aux nôtres (...). Il existe en réalité toutes sortes de situations qui ont du mal à être distinguées* »².

Les Frères musulmans bénéficient en outre de soutiens divers en provenance de l'étranger.

Si un État comme le **Qatar** ne saurait être considéré, selon Olivier Roy, comme un « centre de production idéologique » de ce point de vue, on peut constater que sa diplomatie publique, au travers du média d'État Al Jazeera notamment, est alignée sur les narratifs fréristes (voir *infra*, IV).

En tout état de cause, l'action des Frères musulmans en France et en Europe doit continuer de constituer un point de vigilance majeur. À cet égard, le rapporteur a eu l'occasion d'auditionner le professeur canadien Patrice Brodeur³, dont les travaux portent sur l'évaluation de la puissance globale des Frères musulmans⁴. La méthodologie qu'il a contribué à mettre en place repose sur cinq principaux indicateurs, eux-mêmes déclinés en sous-indicateurs chiffrés, permettant de calculer un indice global. Ces cinq indicateurs sont : l'organisation internationale du mouvement, la puissance politique et sécuritaire, la puissance médiatique, la puissance économique et la puissance sociétale. Ce type de travaux peut constituer une base utile pour appréhender la menace représentée par l'action des Frères musulmans.

Ont également été cités, au cours des différentes auditions conduites par le rapporteur, l'action **d'organisations islamistes issues du Maghreb** tels que les Frères musulmans tunisiens (*Ennahda*) ou encore l'organisation d'origine marocaine Justice et Bienfaisance pour influencer certaines

¹ Florence Bergeaud-Blacker, *Le frériste et ses réseaux, l'enquête*, Odile Jacob, janvier 2023, p. 90.

² [Audition](#) du 4 avril 2024.

³ [Audition du rapporteur](#), 3 juin 2024.

⁴ Il participe aux travaux relatifs à [l'Index de la puissance globale des Frères musulmans](#) menés par le laboratoire d'idées TRENDS, établi aux Émirats arabes unis.

structures islamiques françaises par la voie du financement de mosquées ou d'envoi d'imams.

La **Turquie**, dont le gouvernement se revendique de l'islam politique, s'efforce également de peser sur les instances officielles de l'islam en France dans son souci, mentionné supra, d'encadrer la pratique religieuse de la communauté de ses ressortissants.

C. QUID DE NOS ALLIÉS ?

La question des influences étrangères en provenance de pays alliés peut également être soulevée.

Tout d'abord, il convient de relever que, contrairement à nos adversaires, nos alliés sont des États démocratiques, au service de sociétés ouvertes. Aussi, des courants idéologiques, potentiellement peuvent s'y exprimer librement, et s'efforcer de peser tant sur les débats publics intérieurs qu'à l'étranger.

À ce titre, les services chargés de la lutte contre les ingérences étrangères en France portent une attention particulière aux mouvances complotistes ou de l'extrême-droite dite « alternative » (*alt-right*) issues notamment du monde anglo-saxon, qui peuvent au demeurant porter des narratifs alignés sur les intérêts russes. L'organisation « *Proud Boys* » et la mouvance « QAnon », issues des États-Unis, peuvent notamment être citées.

À l'échelle étatique, l'opération d'influence menée par les États-Unis pour obtenir en janvier 2021 la dénonciation, par l'Australie, du contrat d'armement passé avec la France pour la livraison de sous-marins nucléaires d'attaque rappelle la nécessité de rester vigilant y compris à l'égard de stratégies d'États alliés.

Si les États-Unis constituent un partenaire essentiel pour la France, notamment en matière de renseignement, les auditions menées par la commission d'enquête ont également permis de souligner l'activisme de cet acteur dans le domaine de l'ingérence économique, en recourant notamment à l'arme normative (*lawfare*).

III. LA FRANCE PRISE POUR CIBLE: INVENTAIRE DE NOS VULÉRABILITÉS

A. UNE FRAGILITÉ INHÉRENTE À NOTRE MODÈLE POLITIQUE ET DÉMOCRATIQUE

Les opérations d'influence étrangères peuvent paradoxalement bénéficier des caractéristiques de notre modèle démocratique et libéral, protecteur des droits et des libertés fondamentaux.

D'une part, en droit interne, les articles 10 et 11 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789 garantissent la liberté d'expression et la liberté de la presse. D'autre part, en droit européen, la liberté d'expression est protégée tant par la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 (article 10) que par la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000. La jurisprudence de la Cour européenne des droits de l'homme se montre également protectrice de la liberté d'expression. Cette dernière « *vaut non seulement pour les "informations" ou "idées" accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent l'État ou une fraction quelconque de la population* »¹.

Les discours faux ou trompeurs sont mal appréhendés par ce cadre démocratique protecteur. Par conséquent, les régimes étrangers hostiles à la France s'en saisissent pour diffuser leurs narratifs et dénigrer ce même modèle démocratique. Par respect du pluralisme, les porte-paroles des régimes autoritaires peuvent librement s'exprimer dans les médias, contribuant à leurs stratégies d'influence ainsi que le rappelle Maxime Audinet : « *il y a un exemple qui marque les esprits : je fais ici référence au porte-parole de l'ambassade de Russie, Alexander Makogonov, qui a été interviewé presque une dizaine ou une douzaine de fois sur différentes chaînes d'information en continu où il déroule le discours et le récit officiel russe sur la guerre en Ukraine, y compris en mobilisant des éléments de désinformation. Si je travaillais pour un service de renseignement russe, j'estimerais que c'est une opération d'influence qui réussit parfaitement puisqu'il parvient à diffuser son discours à une heure de grande écoute, à des centaines de milliers de nos concitoyens, et sans toujours être confronté à une contradiction qui soit à la hauteur* ».

Ce dévoiement des valeurs démocratiques et libérales est d'autant plus inquiétant qu'il est opéré par des régimes qui répriment lourdement ces mêmes valeurs dans leurs pays. Outre ce cadre répressif en interne, les régimes autoritaires poursuivent l'objectif de couper leurs populations de toute influence extérieure, perçue comme négative par nature. Cette volonté explique une démarche de fragmentation de l'internet par la Chine et la Russie, afin d'assurer un contrôle total de la diffusion de l'information sur

¹ CEDH, n° 5493/72, 7 décembre 1976, Handyside c. Royaume-Uni.

leurs territoires¹. Dans le même sens, ces États se caractérisent par une absence de réciprocité dans l'ouverture aux médias étrangers. Le régime chinois, engagé dans une expansion de son audiovisuel extérieur depuis 2016, n'autorise qu'au compte-gouttes les médias occidentaux à travailler en Chine.

Par ailleurs, l'instrumentalisation de ces principes de liberté permet à nos concurrents de mettre à l'épreuve notre modèle démocratique. En réponse aux opérations d'influence les plus agressives, les régimes démocratiques peuvent être tentés de recourir à des instruments non démocratiques : « *Avec l'essor de l'intelligence artificielle, les gouvernements soucieux de préserver les institutions démocratiques et la sincérité du vote se trouvent confrontés à des dilemmes cornéliens, tout autant qu'à des questions insolubles. Les démocraties peuvent-elles, en temps de paix, utiliser « les armes de l'adversaire » sans renier leurs valeurs et dévooyer leurs principes ? »*².

Dans le même sens, il paraît hautement complexe, pour un régime démocratique, de déterminer ce qui relève ou non d'un discours faux. Tout au long de ses auditions, la commission d'enquête a pu constater que la tentation d'un « ministère de la vérité » constituait, en matière de désinformation et d'influence, une position à écarter d'emblée. Comme l'a souligné Grégoire Lemarchand, rédacteur en chef de l'investigation numérique à l'Agence France-Presse (AFP) : « *il est beaucoup plus compliqué, ne serait-ce qu'au regard de la liberté d'opinion et de la liberté d'expression, de sanctionner une émission dans laquelle un invité exprime simplement des idées un peu « tordues ». Est-ce à l'Arcom de juger de ce qui est une fausse information ? Je ne le crois pas. La liberté d'expression, c'est une question extrêmement sensible* ».

Au-delà des valeurs démocratiques communes aux pays occidentaux, certains principes spécifiques au modèle républicain peuvent faire de la France la cible potentielle d'opérations d'influence. Le principe de laïcité, qui connaît une application particulière en France, devient un levier pour des campagnes anti-françaises menées depuis l'étranger. Des États compétiteurs de la France peuvent se saisir de l'incompréhension que suscite ce concept pour accuser la France de persécutions religieuses. En 2020, la Turquie a mené ainsi une offensive diplomatique contre la France, accompagnée d'appels au boycott des produits français, suite à la publication de caricatures par le journal *Charlie Hebdo*. Ces dernières avaient été jugées « islamophobes » par le régime turc, dans un contexte de tensions diplomatiques avec la France en Méditerranée orientale. Plus récemment, les opérations d'ingérence émanant d'acteurs pro-Azerbaïdjan ont également exploité la thématique d'une prétendue « islamophobie » inhérente au modèle français de laïcité.

¹ Julien Nocetti, [Un Internet en morceaux ? Fragmentation d'Internet et stratégies de la Chine, la Russie, l'Inde et l'Union européenne, Institut français des relations internationales](#), février 2024.

² Céline Marangé et Maud Quessard, « *Le nouvel âge des guerres de l'information* », in Les guerres de l'information à l'ère numérique, Presses universitaires de France, 2021.

B. UNE EXPOSITION PROPRE À SON STATUT DE SEPTIÈME PUISSANCE MONDIALE

Le statut de la France en tant que septième puissance mondiale et ses prises de position sur la scène internationale contribuent à en faire une cible pour les opérations d'influence étrangères. Les manœuvres d'influence informationnelle apparaissent fréquemment en réaction aux positions de la France. À titre d'exemple, le soutien exprimé par la France à l'Ukraine suite à l'agression russe a conduit à de virulentes opérations d'influence informationnelle. Pareillement, les agissements de l'Azerbaïdjan à l'égard de la France s'inscrivent dans cette logique de rétorsion. Du fait des prises de positions françaises sur le conflit entre l'Arménie et l'Azerbaïdjan, le régime de Bakou s'est engagé dans des campagnes de désinformation particulièrement virulentes et des tentatives d'influence visant les Outre-mer et la Corse. **Caractérisé par un faible coût et une simplicité d'organisation, le recours à ces opérations constitue une « réponse du faible au fort »,** permettant à une petite puissance du Caucase de frapper un État doté. Pour le général Pascal Ianni, directeur du pôle « anticipation stratégique et orientations » à l'état-major des armées : « *C'est l'arme du pauvre, car tout le monde peut pratiquer cette forme d'ingérence qu'est la désinformation, à condition de maîtriser des algorithmes, de savoir créer des contenus et de disposer de relais efficaces. Cette arme touche jusqu'au cœur de notre société* ».

En outre, le déploiement de forces françaises hors du territoire national expose les armées à des opérations d'influence malveillante de la part des grands compétiteurs de la France. Les opérations extérieures font désormais l'objet d'attaques informationnelles adverses. À cet égard, l'expérience de la présence française au Sahel est particulièrement illustrative. Les enjeux informationnels sont progressivement montés en puissance à mesure que la Russie et ses *proxies* s'inséraient dans la zone. Cette présence s'est traduite par des campagnes de désinformation massives de dénigrement des actions de l'armée française, à destination des populations sahéliennes, complexifiant les opérations en cours. **Le risque réputationnel local doit désormais être pris en compte dans la préparation et la conduite de chaque mission extérieure.**

Dans le même sens, **l'organisation par la France de grands événements internationaux constitue pour ses compétiteurs autant d'occasions de dénigrer son modèle et d'abîmer son image à l'international.** Les jeux Olympiques et Paralympiques de Paris (JOP), qui se déroulent en juillet et en août 2024, ont fait l'objet depuis des mois de campagnes de désinformation de la part de la Russie et de l'Azerbaïdjan.

S'agissant de la Russie, une étude du centre d'analyse de la menace de Microsoft a ainsi identifié plusieurs actions de manipulation de l'information menées sur les réseaux sociaux par la Russie et ciblant

l'organisation des JOP¹. Le narratif de ces campagnes reposait sur de faux contenus imitant des communiqués d'institutions publiques ou de médias reconnus et visant à diffuser l'idée d'un risque sécuritaire élevé à Paris. De manière similaire, le ministre délégué chargé de l'Europe, Jean-Noël Barrot, a attribué à la Russie l'amplification de nouvelles alarmistes au sujet de la prolifération des punaises de lit dans la capitale à l'approche des JOP².

Captures d'écran de fausses vidéos alertant sur la dégradation du risque sécuritaire à l'approche des JOP en utilisant des visuels du renseignement américain (à gauche) et de France 24 (à droite)



Source : Centre d'analyse de la menace de Microsoft

Concernant l'Azerbaïdjan, le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) a détecté une ingérence numérique étrangère menée en juillet 2023 et appelant au boycott des JOP de 2024. Viginum a baptisé cette opération de désinformation *Olympiya*³.

¹ Clint Watts, [How Russia is trying to disrupt the 2024 Paris Olympic Games](#), Microsoft Threat Analysis Center, 2 juin 2024.

² TFI info, « [La psychose autour des punaises de lit "amplifiée" par le Kremlin, selon le ministre Jean-Noël Barrot](#) », 1^{er} mars 2024, consulté le 30 juin 2024.

³ RFI, « [Manipulation de l'information sur les JO 2024 à Paris, la piste de l'Azerbaïdjan](#) », 14 novembre 2023, en ligne, consulté le 3 juillet 2024.

Le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum)

Créé par un décret du 13 juillet 2021¹, le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) est un **service à compétence nationale** rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN).

Au préalable, ce décret définit les **ingérences numériques étrangères** comme des opérations impliquant, de manière directe ou indirecte, un État étranger ou une entité non étatique étrangère, et visant à la diffusion artificielle ou automatisée, massive et délibérée, par le biais d'un service de communication au public en ligne, d'allégations ou imputations de faits manifestement inexactes ou trompeuses de nature à porter atteinte aux intérêts fondamentaux de la Nation.

Dans le cadre de sa mission de protection face à ces opérations, Viginum est chargé de :

- détecter et caractériser, en analysant les contenus accessibles publiquement sur les plateformes en ligne, les ingérences numériques étrangères, notamment lorsque celles-ci sont de nature à altérer l'information des citoyens pendant les périodes électorales ;

- assister le Secrétaire général de la défense et de la sécurité nationale dans sa **mission d'animation et de coordination des travaux interministériels** en matière de protection contre ces opérations ;

-fournir toute information utile à l'Arcom dans l'accomplissement des missions qui lui sont confiées par la loi du 30 septembre 1986 susvisée, ainsi qu'à la Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle (CNCEFP) ;

- contribuer aux travaux européens et internationaux et assurer la liaison opérationnelle et technique avec ses homologues étrangers, dans le respect des attributions du ministre des affaires étrangères.

Le pouvoir réglementaire a autorisé Viginum à **mettre en œuvre un traitement informatisé et automatisé de données à caractère personnel**, selon des modalités encadrées². Celui-ci ne peut être effectué qu'aux seules fins de détecter et de caractériser des ingérences numériques étrangères, notamment lorsque ces opérations sont de nature à altérer l'information des citoyens pendant les périodes électorales. Ce traitement repose sur la collecte et l'exploitation des contenus publiquement accessibles aux utilisateurs des plateformes en ligne dont l'activité sur le territoire français dépasse un seuil de cinq millions de visiteurs uniques par mois.

L'activité de Viginum, en particulier au titre de ses prérogatives de traitement automatisé de données, est suivie par un **comité éthique et scientifique**, qui peut adresser au chef du service toute recommandation sur les conditions d'exercice des missions du service.

Source : commission d'enquête

¹ Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères ».

² Décret n° 2021-1587 du 7 décembre 2021 portant autorisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères.

Plus de 1 600 publications ont été diffusées par seulement 91 comptes entre le 26 et le 27 juillet 2023, laissant suggérer une amplification inauthentique. Des erreurs de traduction, des caractères azéris ou de précédentes publications soutenant le parti présidentiel azerbaïdjanaïs ont permis d'identifier qu'une grande partie de ces comptes se rattachait au régime illibéral caucasien. **En sus de cette manœuvre informationnelle fondée sur l'amplification artificielle de contenus sur les plateformes, l'opération s'est également appuyée sur un faux site d'information, Newyorkinsider.**

Par ailleurs, le passé de la France, en particulier son statut de puissance coloniale jusqu'à la seconde moitié du XX^{ème} siècle, est fréquemment utilisé dans le narratif des opérations d'influence. **Il s'agit, pour ses adversaires, de démontrer que la France a conservé ses réflexes coloniaux et qu'elle continue d'exploiter de manière unilatérale les ressources des pays du « Sud global » et de certains de ses propres territoires.**

Ce type de narratif est particulièrement utilisé pour cibler la France sur deux théâtres. **L'Afrique, d'une part, constitue une zone privilégiée pour la diffusion de ces discours.** Les campagnes informationnelles portées par la Russie en Afrique francophone diffusent activement l'image de pays européens uniquement préoccupés par la captation des ressources naturelles africaines. **Les Outre-mer apparaissent, d'autre part, comme un terrain propice au développement de ces éléments de désinformation.**

C. UNE FRAGILITÉ LIÉE À DES FRACTURES POLITIQUES, SOCIALES ET TERRITORIALES, TERREAU FERTILE AUX INFLUENCES MALVEILLANTES

En sus des fractures territoriales, évoquées supra, **chaque épisode de tensions sociales ou politiques constitue un levier potentiel d'influence.** L'un des constats relevés par la commission d'enquête à propos des opérations d'influence est leur profond opportunisme. Si elles s'inscrivent parfois dans des stratégies de long terme de déstabilisation des démocraties pensées par des États autoritaires comme la Russie et la Chine, **elles s'appuient fréquemment sur des opportunités de court terme.**

Ces dernières années, les mouvements sociaux *Occupy Wall Street* ou *Black Lives Matter* aux États-Unis, les manifestations anti-immigration *Pegida* (*Patriotische Europäer gegen die Islamisierung des Abendlandes*) en Allemagne, les Gilets jaunes en France ou les mouvements antivaccins dans l'ensemble des pays occidentaux ont fait l'objet d'opérations extérieures d'amplification. David Colon a ainsi déclaré à la commission d'enquête : « *Le jour où j'ai personnellement, pris conscience [...] de l'interférence du Kremlin dans nos débats publics, c'était en 2018, lors d'une manifestation des Gilets jaunes, l'acte 3, je crois. Alors que je regardais un outil comparable anglo-saxon, celui du German Marshall*

Fund, j'ai pu constater comment, sur Twitter, il y avait eu une manipulation manifestement inauthentique des tendances pour encourager les manifestants à des actes de violence »¹. Plus récemment, les manifestations d'agriculteurs au sein des États membres de l'Union européenne au printemps 2024 ont été l'objet d'opérations d'influence. Nicolas Tenzer a ainsi affirmé, devant la commission d'enquête « non seulement une amplification de la colère des agriculteurs avec peut-être certains groupes un peu plus actifs que d'autres, un peu plus « travaillés » que d'autres, mais aussi un objectif assez direct d'instrumentalisation des protestations »².

Les territoires d'Outre-mer forment également un terrain propice à l'instrumentalisation des tensions sociales et politiques par un discours critique du passé de la France (cf. encadré ci-après).

Outre-mer, Corse : Bakou veut faire payer le prix fort à la France

Les relations entre la France et l'Azerbaïdjan se sont particulièrement distendues depuis la seconde guerre du Haut-Karabagh en septembre 2020.

En riposte au soutien français à l'Arménie, le régime azerbaïdjanais a lancé, outre une campagne informationnelle visant l'organisation des JOP, plusieurs initiatives de soutien aux partis et groupes politiques indépendantistes en Outre-mer et en Corse. Ce soutien s'est notamment traduit par la constitution en juillet 2023 du « Groupe d'initiative de Bakou » (BIG)³, en marge de la conférence du Mouvement des pays non-alignés, et la publication d'une déclaration dans la direction de l'élimination totale du colonialisme. Cette déclaration associait des responsables du Front de libération nationale kanak et socialiste, du parti indépendantiste guyanais Mouvement de décolonisation et d'émancipation sociale, du parti pour la libération de la Martinique, du Mouvement des démocrates et des écologistes pour une Martinique souveraine et du parti polynésien Tāvini huiraatira.

Le mouvement indépendantiste corse Nazione s'est par la suite joint au BIG. L'Azerbaïdjan, dans sa démarche d'influence malveillante, tente également de capitaliser sur les tensions entre l'État français et les partis autonomistes et indépendantistes corses. Des journalistes de l'agence de presse azerbaïdjanaise Azertac ont couvert différentes manifestations sur l'île avec l'intention manifeste d'adopter un prisme anti-français. Pour autant, ces manœuvres ne paraissent pas avoir prospérées. Lors de son audition par la commission d'enquête, le ministre de l'intérieur et des Outre-mer a indiqué « En Corse, par exemple, l'Azerbaïdjan a effectué des tentatives d'ingérence, suite à l'assassinat d'Yvan Colonna et des émeutes qui s'en sont suivies, sans rencontrer, là encore, une grande efficacité »⁴.

Des partenariats plus poussés ont été par la suite noués entre les mouvements indépendantistes kanaks et l'Azerbaïdjan. En avril 2024, une élue indépendantiste a signé un mémorandum au nom du président du Congrès de la Nouvelle-Calédonie, scellant la mise en place d'une coopération avec le Parlement d'Azerbaïdjan⁵.

¹ [Audition](#) du 29 février 2024.

² *Idem*.

³ Pour Baku Initiative Group.

⁴ [Audition](#) du 28 mai 2024.

⁵ Mathurin Derel, « [Nouvelle-Calédonie : un accord parlementaire avec l'Azerbaïdjan suscite l'incompréhension](#) », *Le Monde*, 26 avril 2024, en ligne, consulté le 3 juillet 2024.

De plus, en décembre 2023, deux ressortissantes azerbaïdjanaises, connues des services de renseignement se présentant comme journalistes ont été expulsées de Nouvelle-Calédonie en marge de la visite du ministre des armées, Sébastien Lecornu¹.

À l'occasion de la crise en Nouvelle-Calédonie, **Viginum a détecté les 15 et 16 mai 2024 deux opérations de diffusion massive et coordonnée de contenus manifestement inexacts ou trompeurs accusant la police française de meurtres** lors des manifestations². Les deux manœuvres visaient à propager des visuels présentant la police française comme responsable de la mort de plusieurs manifestants.

Ces manœuvres se sont largement appuyées sur des accusations de colonialisme ou de néocolonialisme. Plusieurs visuels diffusés sur les réseaux sociaux, en anglais et en français : « *La police française est meurtrière. Les meurtres des algériens continuent...* ». Ces références à la guerre d'Algérie visaient à assimiler les opérations de maintien de l'ordre face aux émeutes aux épisodes de répression sanglante de manifestations algériennes. Les mots clés #EndFrenchColonialism et #FrenchColonialism accompagnaient fréquemment les messages relayés. Plusieurs visuels ont également associé des codes issus de la campagne *Olympiya*, visant l'organisation des jeux Olympiques et Paralympiques de Paris.

Capture d'écran d'un visuel accusant la police française du meurtre de manifestants néo-calédoniens



Source : Viginum

¹ Europe 1, « *Indopacifique : l'Azerbaïdjan a mené une opération de déstabilisation lors de la visite de Sébastien Lecornu en Nouvelle-Calédonie* », 12 décembre 2023, en ligne, consulté le 3 juillet 2024.

² Viginum, *Sur X et Facebook, plusieurs manœuvres informationnelles d'origine azerbaïdjanaise ciblent la France dans le contexte des émeutes en Nouvelle-Calédonie*, fiche technique, 17 juin 2024.

Viginum a identifié les auteurs de ces actions comme des comptes liés au régime azerbaïdjanaise. Sur les 301 comptes détectés par le service, 112 d'entre eux comprenaient des éléments biographiques les reliant au parti présidentiel *Yeni Azərbaycan Partiyası* (YAP).

Source : commission d'enquête d'après Viginum

Constater cette instrumentalisation des mouvements sociaux et des épisodes de tensions par des tentatives d'influence étrangères **ne revient pas à nier ni la réalité ni la légitimité de ces protestations**. Les influences étrangères ont peu d'effet sur le déclenchement de ces mouvements ; **elles jouent sur les colères en tentant de les encourager et de les accentuer**. Si l'efficacité et la portée de ces manœuvres demeurent incertaines, leurs objectifs sont transparents : « *appuyer là où cela fait mal* », accentuer les dissensions internes, déstabiliser nos démocraties et *in fine* démontrer l'infériorité de ce modèle.

Il importe de garder en mémoire que **les politiques publiques de réponse aux opérations d'influence ne pourront traiter les causes profondes de ces mouvements** de protestations ou des fractures politiques et sociales qui nécessitent des réponses structurelles dépassant largement le cadre de la commission d'enquête. En revanche, **il est prudent de conjecturer que chaque thématique potentiellement porteuse de tensions pourra faire l'objet de tentatives d'instrumentalisation**.

Cette logique est limpide décrise par Giuliano da Empoli dans son roman *Le Mage du Kremlin*. L'auteur y décrit, par l'intermédiaire de Vadim Baranov, narrateur inspiré du conseiller de Vladimir Poutine Vladislav Sourkov, la stratégie informationnelle russe : « *Nous ne devons convertir personne, Evgueni, juste découvrir ce en quoi ils croient et les convaincre encore plus, tu comprends ? Donner des nouvelles, de vrais et de faux arguments, cela n'a pas d'importance. Les faire enrager. Tous. Toujours plus. Les défenseurs des animaux d'un côté et les chasseurs de l'autre. Ceux du Black Power d'un côté et les suprémacistes blancs de l'autre. Les activistes gays et les néonazis. Nous n'avons pas de préférence, Evgueni. Notre seule ligne, c'est le fil de fer. Nous le tordons d'un côté et nous le tordons de l'autre. Jusqu'à ce qu'il se casse* »¹.

D. UNE FRAGILITÉ DÉCOULANT DU DÉSARMEMENT DE L'ÉTAT

Les fragilités de l'État et de nos politiques publiques forment également un terreau favorable aux influences étrangères. L'effet conjugué des contraintes budgétaires et d'une prise de conscience tardive du durcissement des stratégies d'influence étrangères a conduit à deux mouvements cumulatifs.

¹ Giuliano da Empoli, *Le Mage du Kremlin*, Gallimard, 2022.

D'une part, ce désarmement budgétaire rend certaines entités publiques plus vulnérables aux opérations d'influence. C'est tout particulièrement le cas des établissements d'enseignement supérieur et de recherche. Le monde de la recherche est affecté depuis des années par un sous-financement alarmant. Ce besoin chronique de ressources expose les établissements à des interférences étrangères. Si les partenariats internationaux forment des sources de financements attractives, ils n'en constituent pas moins des leviers d'influence considérables pour des puissances étrangères. Le manque de moyens, doublé d'une faible reconnaissance du rôle et de la place des chercheurs dans la société a, par ailleurs, pu conduire à un affaiblissement de notre niveau de connaissance du phénomène des influences étrangères.

D'autre part, ce désarmement affaiblit la propre politique d'influence de la France. Les instruments de la diplomatie d'influence se sont en effet réduits au cours des dernières années.

Parmi les leviers de l'influence française à l'étranger, les instituts de recherche français, comme le Centre d'études et de documentation économiques, juridiques et sociales (CEDEJ) du Caire, à l'Institut français du Proche-Orient (IFPO) et l'Institut de recherche sur l'Asie du Sud-Est contemporaine (IRASEC), à Bangkok, ont aujourd'hui des budgets limités. Le professeur Charillon a souligné en ce sens que « *Cet extraordinaire instrument d'influence risque d'être un jour repris en main par des financements étrangers. En conséquence, on a un certain nombre d'atouts que l'on délaisse parce que l'on refuse de les assumer comme instruments d'influence et qui risquent de devenir des instruments d'influence des autres, en France* ».

E. UNE FRAGILITÉ DU CITOYEN

1. Une fragilité de l'« *individu démocratique* »

Une grande part du succès des opérations d'influences étrangères repose sur le niveau de résilience de la société. À cet égard, la sensibilité des individus aux opérations d'influence, et en premier lieu aux opérations de manipulation de l'information, est déterminante. Les citoyens sont en effet les premières cibles de ce type d'opérations, qui tentent d'orienter l'opinion publique.

Selon le chercheur Laurent Cordonier, auditionné par la commission d'enquête « les plus « belles » campagnes de désinformation ou d'ingérence, les plus fines, les mieux équipées en termes d'intelligence artificielle ou de deepfake ne peuvent avoir prise que sur une population dont le système immunitaire cognitif n'est pas assez développé et qui présente donc des facteurs de risque en constituant un terrain favorable, prêt à accepter ces désinformations »¹. Trois

¹ [Audition](#) du 7 mars 2024.

facteurs principaux déterminent le niveau de sensibilité des individus aux opérations de désinformation.

Premièrement, certains mécanismes psychosociaux favorisent la propagation et l'assimilation des fausses nouvelles. Tout d'abord, les individus sont plus susceptibles de croire une information qui vient confirmer ou conforter leurs positions préalables, en application d'un « biais de confirmation ». Ensuite, les fausses nouvelles sont généralement présentées de manière à surprendre et à susciter l'intérêt. Dans le cadre des campagnes de manipulation de l'information en ligne, elles sont conçues pour avoir une viralité importante et être diffusées le plus largement possible. Enfin, les styles de pensée des individus peuvent affecter leur perméabilité à la désinformation¹. Les sciences cognitives ont ainsi identifié deux styles de pensée distinct. Le premier est un style de pensée « intuitif ». Or, pour Laurent Cordonier, les personnes intuitives « se fient avant tout à leur intuition ou à leur première impression pour savoir si cette information est vraie ou non et si elles doivent lui accorder du crédit »². À l'inverse, le style de pensée analytique mobilise un système de traitement de l'information plus rigoureux. Les personnes dites analytiques sont plus enclines à réviser une intuition initiale erronée. Cette distinction entre les styles de pensée n'est pas absolue et chaque individu peut être successivement intuitif ou analytique.

Deuxièmement, l'éducation des individus et leur niveau de connaissances préalables d'un sujet peuvent renforcer leur niveau de résilience. À titre d'exemple, selon une étude de la Fondation Descartes, les personnes disposant d'un plus faible niveau de connaissances scientifiques étaient plus enclines à croire des informations fausses sur la pandémie de Covid³. Des connaissances scientifiques de base conduisent les individus à plus facilement rejeter les théories du complot.

Troisièmement, la défiance des citoyens à l'égard des médias traditionnels et des institutions est un facteur important de diffusion des fausses informations. En ce sens les travaux de David Chavalarias, directeur de recherche au CNRS, ont identifié que les personnes les plus marquées par une défiance à l'égard des médias et des institutions sont les plus susceptibles de relayer de fausses informations, y compris lorsqu'elles sont contradictoires ou ont peu de liens entre elles⁴. Les personnes ayant reposté des messages de désinformation autour du Covid-19 se retrouvent ainsi parmi les relais de la propagande russe.

Or, selon un sondage réalisé pour le Cevipof, la France se caractérise par un plus fort niveau de rejet de la politique que d'autres pays de l'Union

¹ [Rapport de la commission « Les Lumières à l'ère Numérique »](#), janvier 2022.

² [Audition](#) du 7 mars 2024.

³ Laurent Cordonier, [Information et santé. Analyse des croyances et comportements d'information des Français liés à leur niveau de connaissances en santé, au refus vaccinal et au renoncement médical](#), Fondation Descartes, novembre 2023.

⁴ [Audition](#) du 4 juin 2024.

européenne. En effet, ce niveau de défiance s'élève à 70 % en France contre 55 % en Allemagne et 46 % en Pologne¹. De plus, ce niveau de défiance s'inscrit en hausse depuis plusieurs années : 68 % des personnes interrogées estiment que la démocratie ne fonctionne pas bien contre 48 % en 2009. Toutefois, à une échelle plus élevée, les travaux de chercheurs ont souligné que plus le secteur public d'un pays est corrompu, plus l'adhésion de sa population à diverses théories du complot hétérogène est forte.

La diffusion de fausses informations peut également prospérer sur l'affaiblissement de l'environnement informationnel. La crise des normes qui affecte le secteur de la presse encourage cette diffusion. **Les médias traditionnels se trouvent concurrencés par les réseaux sociaux** où la présentation des informations se fait sans respect des standards du journalisme. Pour autant, si la confiance dans les médias se situe à un niveau faible en France (28 %), mais relativement similaire à ce qui prévaut en Allemagne (34 %), en Italie (26 %) et en Pologne (25 %), elle demeure supérieure à la confiance accordée aux réseaux sociaux. Ces derniers ne recueillent que 16 % de confiance de la part des personnes interrogées. **À la crise des normes du secteur de la presse s'ajoute une crise du modèle économique.** La baisse des revenus publicitaires combinée à la concurrence des réseaux sociaux a conduit à une réduction drastique des recettes de la presse traditionnelle, dont les moyens d'investigation s'en trouvent conséquemment affaiblis. Comme le relevait l'Ambassadeur pour le numérique, Henri Verdier, lors de son audition : « *Il y a trente ans, un tiers des revenus du secteur provenait des petites annonces, qui sont maintenant parties vers les sites web ; le deuxième tiers provenait de la publicité, sur laquelle quelques géants numériques ont pris un quasi-monopole en imposant leurs tarifs ; enfin le troisième tiers provenait des abonnements, qui sont devenus la seule source de revenus [...] La perte de crédibilité, de puissance et d'autonomie de la presse fait donc partie du problème auquel nous sommes confrontés* »².

2. La fragilité des décideurs publics et privés

Une grande partie des élus, locaux comme nationaux, ainsi que des hauts fonctionnaires et des dirigeants du secteur privé **n'ont encore qu'une conscience limitée de la menace des influences étrangères malveillantes**. Le rapport public de la délégation parlementaire au renseignement de juin 2023 précitait déjà une forme de « naïveté » chez ces décideurs³.

Tout d'abord, s'agissant des élus, la sensibilisation aux questions d'influence paraît lacunaire. **Les élus locaux, en particulier, sont peu au fait**

¹ Sondage Opinionway pour Sciences Po, [Baromètre de la confiance politique – vague 15](#), janvier 2024.

² [Audition](#) du 28 mars 2024.

³ [Rapport public n° 1454 \(seizième législature- Assemblée nationale\) / n° 810 \(2022-2023 – Sénat\)](#) fait par Sacha Houlié au nom de la délégation parlementaire au renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023, déposé le 29 juin 2023.

des risques qui pèsent sur les collectivités territoriales. Les décideurs locaux peuvent cependant apparaître comme de potentiels relais d'influence pour des puissances étrangères. L'échelon local est en effet une cible plus discrète et accessible. **Des États étrangers peuvent viser l'obtention d'avantages économiques, au travers de la commande publique des collectivités territoriales**, ou de quadrillage d'un territoire précis, par des investissements ciblés et des partenariats avec le monde associatif, en menant des opérations d'influence auprès des élus locaux.

Concernant les fonctionnaires, ensuite, la conscience de la menace des influences étrangères diminue hors des domaines régaliens. Pourtant, les secteurs de la santé ou de l'enseignement supérieur et de la recherche constituent des cibles privilégiées pour des opérations d'influence. Si les récents travaux du Sénat, en particulier le rapport d'André Gattolin au nom de la mission d'information sur les influences étrangères extra-européennes dans le monde universitaire¹, ont permis d'alerter sur le défaut de sensibilisation existant au sein des universités, pour autant, la culture d'ouverture vers l'international et de diffusion des connaissances académiques, conjuguée à des opportunités de financements extérieurs, prime encore sur la vigilance à l'égard d'intentions malveillantes.

Enfin, pour les chefs d'entreprises, la problématique des influences étrangères est encore peu identifiée. **De nombreuses entreprises ne perçoivent pas que nouer des coopérations** ou vendre une partie de leurs activités à des partenaires étrangers peut présenter un risque pour la sécurité de notre pays. Cette fragilité est d'autant plus problématique qu'elle peut concerner les entreprises et sous-traitants de la base industrielle et technologique de défense (BITD).

IV. LUTTE INFORMATIONNELLE, CAPTURE DES ÉLITES, CONTRÔLE DES DIASPORAS... : TYPOLOGIE DES MODES OPÉRATOIRES

A. LES OPÉRATIONS DE LUTTE INFORMATIONNELLE

La part la plus visible des opérations d'influence étrangères correspond aujourd'hui aux opérations de désinformation. **La Commission européenne, dans une communication de 2018, a défini la désinformation comme** « les informations dont on peut vérifier qu'elles sont fausses ou trompeuses, qui sont créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public et qui sont susceptibles de causer un préjudice public. Par préjudice public on entend les menaces aux processus politiques et d'élaboration

¹ [Rapport d'information n° 873 \(2020-2021\)](#), fait par André Gattolin au nom de la mission d'information du Sénat sur les influences étrangères extra-européennes dans le monde universitaire et académique français et leurs incidences, déposé le 29 septembre 2021.

des politiques démocratiques et aux biens publics, tels que la protection de la santé des citoyens de l'Union, l'environnement ou la sécurité »¹.

Au niveau français, le ministère de l'Europe et des affaires étrangères, au travers du Centre d'analyse, de prévision et de stratégie (Caps) définit les opérations de manipulation de l'information comme « *la diffusion intentionnelle et massive de nouvelles fausses ou biaisées à des fins politiques hostiles* »².

1. Les acteurs de la guerre informationnelle

Dans ce cadre de lutte informationnelle, plusieurs outils peuvent être mobilisés par les États hostiles à la France et ses alliées, en particulier :

- les **institutions publiques**, au premier rang desquelles se situent le réseau diplomatique et les services de communication des différents ministères et administrations publiques. Dans le cas de la Chine, ces instances gouvernementales se doublent de celles du Parti communiste chinois (PCC) ;
 - les **services de renseignement**, dont les opérations clandestines peuvent poursuivre des visées d'influence ;
 - les **agences de presse ou les groupes médiatiques** liés à des États ;
 - les proxys, groupes para-étatiques, prestataires privés et ONG, formant une **nébuleuse de relais d'influence**, et pouvant mener des actions pour le compte d'un État sans pouvoir y être directement rattachés ;
 - les ***think tanks* et instituts de recherche**, dont l'action de soutien à la politique d'influence se manifeste plus particulièrement dans le domaine de l'enseignement supérieur et de la recherche et qui sera développé *infra*.

a) La communication des diplomatises

Les opérations d'influence peuvent s'appuyer sur les différents acteurs qui concourent à la diplomatie publique des États compétiteurs de la France. Pour mémoire, la diplomatie publique est définie par Frédéric Charillon comme un ensemble d'actions « consistant à la fois à promouvoir publiquement le contenu de la diplomatie d'État, et à prendre contact directement avec des publics, sans passer par leurs autorités politiques »³. Cette mise à disposition de l'appareil étatique et para-étatique au service d'une lutte informationnelle est particulièrement marquée s'agissant de la Russie. La

¹ Commission européenne, Lutter contre la désinformation en ligne : une approche européenne, communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 26 avril 2018.

² Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, « Les manipulations de l'information. Un défi pour nos démocraties », Rapport du Centre d'analyse, de prévision et de stratégie (Caps) du ministère de l'Europe et des affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (Irsem) du ministère des armées, Paris, août 2018.

³ Frédéric Charillon, « Chapitre IV. Les politiques d'influence », Maurice Vaisse éd., Diplomatie française. Outils et acteurs depuis 1980, Odile Jacob, 2018, pp. 381-394.

Chine, engagée dans une démarche de « *russianisation* » de ses opérations d'influence, selon les termes de Paul Charon et de Jean-Baptiste Jeangène Vilmer¹, place désormais également ses outils de diplomatie publique dans une optique informationnelle.

Traditionnellement, les activités de diplomatie publique poursuivent un objectif de promotion de l'image du pays concerné. Le durcissement des stratégies d'influence opéré par les États a réorienté ces activités vers un dénigrement du modèle occidental et de défense agressive de leurs intérêts dans l'espace informationnel.

S'agissant de la mobilisation des institutions publiques, la « *diplomatie du loup guerrier* » ou « *diplomatique du loup combattant* » menée par le ministère chinois des affaires étrangères est **topique d'un durcissement de la diplomatie publique de la République populaire de Chine**. Cette stratégie, qui repose sur un discours particulièrement virulent à l'égard des discours critiques des intérêts chinois, s'est **accélérée à la suite de la pandémie de Covid-19 en 2020**. Comme le relève le rapport de l'Irsem, si les diplomates chinois ont recours aux outils classiques des relations publiques (communiqués, courriers, conférences de presse...), leurs activités s'étendent aussi à la sphère numérique et aux réseaux sociaux. **Dans une forme de « *trollisation* » de la diplomatie chinoise, les fonctionnaires des ambassades peuvent interpeller violemment** des chercheurs, élus ou journalistes émettant des critiques sur la Chine.

En France, la **diplomatie du loup guerrier** a été incarnée ces dernières années par l'ambassadeur de Chine en France Lu Shaye, volontiers provocateur et n'hésitant pas à cibler de ses diatribes numériques des ressortissants français². En avril 2020, l'ambassadeur avait été convoqué par la ministre de l'Europe et des affaires étrangères Catherine Colonna pour une déclaration accusant les personnels des Ephad d'abandon de postes en pleine crise sanitaire. De manière plus ciblée, Lu Shaye a adressé au chercheur Antoine Bondaz une série de tweets imagés le qualifiant de « *petite frappe* », de « *troll idéologique* » et de « *hyène folle* »³.

Concernant la Russie, les **porte-parolats des administrations russes n'hésitent pas davantage à annoncer et diffuser de fausses informations**, combinant ces annonces avec des manœuvres informationnelles numériques. Le 17 janvier 2024, le ministère russe de la défense a ainsi annoncé la mort de 60 « *mercenaires français* » dans une frappe sur la ville ukrainienne de

¹ Paul Charon et Jean-Baptiste Jeangène Vilmer, « *Les Opérations d'influence chinoises. Un moment machiavélien* », rapport de l'Institut de recherche stratégique de l'École militaire (Irsem), Paris, ministère des armées, septembre 2021 – rapport téléchargeable [ici](#).

² Romain Geoffroy et Dorian Jullien, « *Lu Shaye, l'ambassadeur de Chine à Paris, un habitué des propos polémiques* », Le Monde, 24 avril 2023 [consulté le 28 juin 2024], en ligne :

https://www.lemonde.fr/les-decodeurs/article/2023/04/24/lu-shaye-l-ambassadeur-de-chine-a-paris-un-habitue-des-propos-polemiques_6170845_4355770.html

³ France 24, « *Quand l'ambassade de Chine se déchaîne contre un chercheur français* », 22 mars 2021, en ligne, consulté le 1^{er} juillet 2024.

Kharkiv. Suite à cette première annonce, l'ambassadeur de France en Russie est convoqué par le ministère des affaires étrangères. Le 22 janvier 2024, **une fausse liste présentant les noms des préputés « mercenaires » français** est diffusée sur des chaînes Telegram russes¹. Ce faux document a été immédiatement relayé par les réseaux d'information russes et les médias d'État. **Comme détaillé *infra* dans la deuxième partie, un travail de vérification des noms a été rapidement engagé par les services de renseignement et le ministère des armées, qui a promptement démenti cette information.**

b) L'action des services de renseignement ou la « clandestinisation » des opérations informationnelles

Les services de renseignement étrangers, au travers de leurs activités clandestines, peuvent mener des opérations d'influence. L'étendue de ces opérations est difficile à mesurer. Toutefois, les auditions menées par la Commission d'enquête ont souligné un regain d'activité des services étrangers sur le sol français.

Cet activisme croissant se manifeste tout particulièrement s'agissant des services russes, **en dépit d'un recul de la présence d'opérateurs du renseignement russe sur le territoire français.** Les contre-mesures diplomatiques et les expulsions d'agents de renseignement sous couverture diplomatique décidées après le déclenchement de l'agression russe contre l'Ukraine ont été suivies d'opérations plus visibles. **Sortant du champ strict de l'espionnage, ces services ont mené des opérations clandestines à visée d'influence, destinées à toucher directement l'opinion publique française.** Il s'agit, comme le souligne Julien Nocetti, d'une forme de « *clandestinisation de plus en plus marquée des stratégies informationnelles hostiles* »².

Selon Maxime Audinet « *ces opérations s'inspirent de ce qu'on appelait à l'époque de la guerre froide les « mesures actives » du FSB qui étaient également des actions d'influence et d'intoxication ciblées sur le camp capitaliste de l'époque* »³. Les archives du KGB transmises par le transfuge Vassili Mitrokhine définissent ces « mesures actives » comme des « *mesures opérationnelles destinées [non seulement] à exercer une influence profitable sur les éléments les plus dignes d'intérêt de la vie politique d'un pays cible, sur sa politique étrangère, sur la résolution de problèmes internationaux, [mais aussi] à induire l'adversaire en erreur, à saper et à affaiblir ses positions, à perturber ses plans hostiles* »⁴.

Quatre opérations menées en région parisienne au cours des derniers mois peuvent être citées. Si des enquêtes judiciaires sont toujours en

¹ RFI, « [Comment la Russie a faussement annoncé la mort de « mercenaires » français en Ukraine](#) », 26 janvier 2024, en ligne, consulté le 4 juillet 2024.

² [Audition](#) du 4 juin 2024.

³ [Audition](#) du 7 mars 2024.

⁴ Vassili Mitrokhine, KGB Lexicon: The Soviet Intelligence Officer Handbook, 2002.

cours, il paraît vraisemblable que ces actions aient été menées par les services de renseignement russes. Il s'agit ainsi notamment :

- **de l'affaire dite « des étoiles de David », au mois d'octobre 2023** avec une série d'étoiles bleues de David taguées à Paris et en Ile-de-France ;

- **des mains rouges sur le mémorial de la Shoah**, peintes dans la nuit du 13 au 14 mai 2024 sur le mur des Justes et renvoyant au massacre de deux soldats israéliens lors de la seconde Intifada en 2000 par une équipe de ressortissants bulgares ;

- **de messages peints au pochoir fin mars dans le quartier de Notre-Dame** indiquant « *Attention ! Chute possible du balcon* », en référence à une alerte sur le danger de balcons surchargés lors des jeux Olympiques et Paralympiques (JOP), par un groupe de moldaves soupçonnés par la préfecture de police d'être commandités par la Russie¹ ;

- **de cinq cercueils de taille réelle** déposés aux abords de la tour Eiffel le 1^{er} juin 2024, recouverts d'un drapeau français et de l'inscription « *soldats français de l'Ukraine* » et remplis de sacs de plâtre.

Dépôt de cercueils marqués de l'inscription « *soldats français de l'Ukraine* » aux abords de la tour Eiffel



Source : Le Parisien

¹ France Info, « Tags de "mains rouges" sur le Mémorial de la Shoah : les enquêteurs privilégièrent l'hypothèse d'une opération de déstabilisation venue de Russie », 21 mai 2024, en ligne, consulté le 3 juillet 2024.

L'affaire des étoiles de David : des « mesures actives » en plein Paris

Au mois d'octobre 2023, quelques jours après l'attaque du 7 octobre, des étoiles de David bleues, peintes au pochoir, sont retrouvées sur les murs de plusieurs endroits de Paris et de villes d'Île-de-France¹. Réalisées par deux équipes distinctes, l'une opérant dans le 10^e arrondissement dans la nuit du 26 octobre et l'autre dans les 14, 15 et 18^e arrondissements, en Seine-Saint-Denis et dans les Hauts-de-Seine, les étoiles peintes suscitent immédiatement l'émotion et la surprise dans le contexte des attaques du Hamas. Un total de 250 tags sera retrouvé sur les murs franciliens.

D'abord assimilée à un acte antisémite, cette action va rapidement être associée à la Russie. Selon les éléments rendus publics par la préfecture de police et l'enquête de la cellule investigation de Radio France², le profil des premières personnes interpellées fait émerger l'hypothèse d'une manipulation des services russes. Les membres des deux équipes, ressortissants moldaves, affichent dans leur pays d'origine des opinions et un activisme prorusse.

S'appuyant sur les travaux de Viginum, le ministère de l'Europe et des affaires étrangères a publié le 9 novembre 2023 un communiqué condamnant une ingérence numérique russe³. Une opération d'amplification des images des étoiles de David sur les murs de Paris a en effet été menée par le russe *Recent Reliable News* (RRN/*Doppelgänger*). Viginum a recensé l'implication d'un réseau de 1 095 bots sur la plateforme X (ex-Twitter), ayant publié 2 589 posts contribuant à la polémique. Le service attribue avec un « haut degré de confiance » cette activité au réseau RRN.

Le lien entre l'amplification de ce contenu et la réalisation de l'opération de terrain par les opérateurs moldaves paraît établi par la chronologie de diffusion des images des étoiles de David. Alors que la première photo authentique des murs tagués apparaît sur les réseaux sociaux le 30 octobre à 19h37, les publications du réseau RRN remonte au 28 octobre à 19h24.

Source : commission d'enquête d'après Viginum et la cellule d'investigation de Radio France

c) Le rôle des médias d'État

Dans une perspective de diplomatie publique, l'audiovisuel extérieur constitue un vecteur essentiel d'influence. Néanmoins, dans un contexte de guerre informationnelle, cet instrument peut être mobilisé au service de stratégies de désinformation et de dégradation de l'image de l'adversaire.

¹ Saint-Ouen et Saint-Denis en Seine-Saint-Denis, d'une part, Issy-les-Moulineaux, Fontenay-aux-Roses et Vanves dans les Hauts-de-Seine, d'autre part.

² Maxime Tellier, « [Étoiles de David taguées à Paris : l'opération était orchestrée par des réseaux russes](#) », [cellule investigation de Radio France](#) », 26 janvier 2024.

³ Ministère de l'Europe et des affaires étrangères, [Russie – Nouvelle ingérence numérique russe contre la France](#), 9 novembre 2023.

Concernant le rôle des médias dans les opérations d'influence, les actions des organes de presse russes contrôlés par le Kremlin représentent un cas d'école.

Deux piliers principaux constituent l'audiovisuel extérieur de la Russie¹. D'une part, l'agence RT a été créée en 2005 sous le nom de *Russia Today* en réaction à l'émergence des « révoltes de couleurs » dans l'ancien espace soviétique. D'autre part, l'agence *Sputnik*, branche internationale *Rossia Segodnia*, lancée en 2014 dans le contexte de la première crise ukrainienne. **Ces deux structures, dotées respectivement d'un budget de 330 et de 92 millions d'euros en 2020, affichent le même positionnement à l'international.** Elles s'affirment comme des médias « alternatifs » au discours de l'Occident libéral. Leurs lignes éditoriales s'inscrivent dans une parfaite cohérence avec les positions internationales de la Russie. Ainsi, la dirigeante *de facto* de ces deux agences, Margarita Simonyan, dans une célèbre et transparente déclaration a indiqué le 18 février 2021 : « *Nous travaillons pour l'État, nous défendons notre patrie, comme le fait par exemple l'armée* ». En dépit de cet alignement sur la diplomatie russe, les deux chaînes se caractérisent par une grande plasticité de leurs contenus, qui rebondissent sur toute actualité susceptible de dénigrer l'adversaire.

La diffusion de RT et Sputnik dans les pays occidentaux a rapidement conduit à des tensions avec les pouvoirs publics. Pour mémoire, à l'occasion de la conférence de presse commune entre les présidents français et russe le 29 mai 2017, le président de la République avait estimé, à propos de ces deux médias, que : « *Quand des organes de presse répandent des contrevérités infamantes, ce ne sont plus des journalistes, ce sont des organes d'influence* ». En octobre 2017, la chaîne RT America a été inscrite comme « agent étranger » au titre du *Foreign Agents Registration Act* par le Département américain de la justice².

Les sanctions portées à l'égard de ces deux médias, détaillées *infra*, n'ont toutefois pas mis fin à leur diffusion. Interrogé par la commission d'enquête, Maxime Audinet a confirmé le redéploiement des versions françaises de RT et Sputnik au travers de deux mouvements. En premier lieu, RT et Sputnik **ont fragmenté leurs infrastructures numériques et, par une technique de sites miroirs**, ont tenté de reconstituer leurs audiences en contournant les mesures restrictives. Si les audiences françaises ne sont pas remonté : « *Une dizaine de sites miroirs en version allemande de RT ont été créés et, aujourd'hui, ils ont au moins autant voire plus d'audience qu'avant l'invasion de l'Ukraine, avec environ cinq à sept millions de visites de leur site par mois : ce sont donc des méthodes qui peuvent fonctionner* »³. En second lieu, **les formats**

¹ [Audition](#) du 7 mars 2024.

² [Reuters](#), *Russia's RT America registers as 'foreign agent' in U.S.*, 13 novembre 2017, consulté le 30 juin 2024.

³ [Audition](#) du 7 mars 2024.

francophones des médias russes se sont réorientés vers l'Afrique. *Sputnik France*, dissous, a été recréé en tant que *Sputnik Afrique*.

Une stratégie similaire a pu être constatée s'agissant des médias d'État chinois, dont l'expansion internationale contribue à la diffusion d'une propagande chinoise largement assumée. À compter de 2016, le régime chinois a structuré un groupe audiovisuel extérieur, le *China Global Television Network* (CGTN), en s'appuyant sur les infrastructures de la télévision d'État CCTV et les contenus produits par l'agence de presse *Xinhua*¹. Une même volonté de diffusion internationale s'est manifestée dans les grands journaux (*China Daily*, *People's Daily*, *Global Times*...) et médias radiophoniques chinois (Radio Chine internationale). L'ensemble de ces médias relaie massivement des éléments de propagande chinoise. Paul Charon indique ainsi que : « *Sur le média extérieur chinois China Global Television Network (CGTN), la majorité des contenus, même francophones, portent sur les États-Unis ou sur la démocratie. L'ambition est de démonétiser l'idée de démocratie, elle-même, pour qu'elle ne soit pas une alternative pour les Chinois ou les populations francophones dans le monde* »².

De manière révélatrice, l'autorisation de diffusion de CGTN France le 3 mars 2021 s'est accompagnée, dès la fin du mois, par l'affaire « Laurène Beaumond »³. CGTN France avait ainsi publié deux articles, sur Taïwan et le Xinjiang, hostiles au discours critique de l'action de la Chine et rédigés par une employée française de la chaîne sous pseudonyme⁴.

Outre l'extension de leur diffusion à l'étranger, les médias chinois investissent directement les journaux étrangers à l'aide de publireportages et de publicités ciblées. Dans un rapport consacré à l'information en Chine, RSF a plus spécifiquement la « *stratégie du Cheval de Troie* » menée auprès de journaux occidentaux et japonais par le média *China Watch*⁵. Ce quotidien de propagande aurait ainsi une audience de plus de 13 millions d'exemplaires au travers d'articles insérés dans des titres de presse reconnus comme le *New York Times*, le *Wall Street Journal*, le *Daily Telegraph*, *El País* ou *Le Figaro*.

¹ Jean-Baptiste Jeangène Vilmer, Alexandre Escoria, Marine Guillaume, Janaina Herrera, « [Les manipulations de l'information. Un défi pour nos démocraties](#) », rapport du Centre d'analyse, de prévision et de stratégie (Caps) du ministère de l'Europe et des affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (Irsem) du ministère des armées, Paris, août 2018.

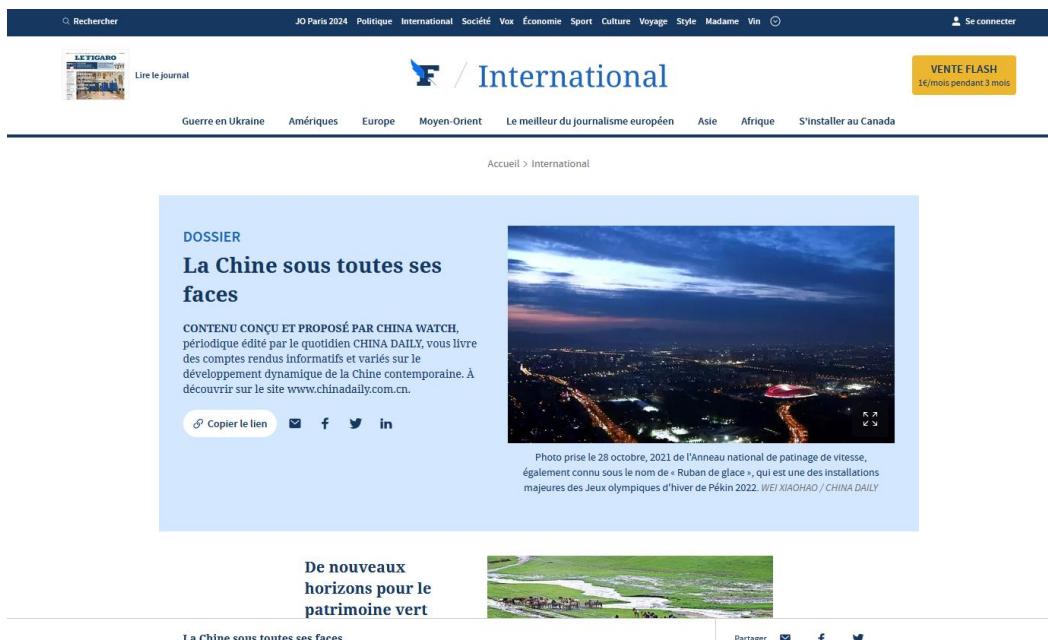
² [Audition](#) du 6 juin 2024.

³ Idem.

⁴ Libération, CheckNews, « [La chaîne chinoise CGTN a-t-elle inventé une journaliste française ?](#) », 2 avril 2021, consulté le 30 juin 2024.

⁵ RSF, [Le nouvel ordre mondial de l'information selon la Chine](#), 2019.

Rubrique du site internet du Figaro proposant un contenu conçu et financé par le *China Watch*



The screenshot shows the Figaro International website. At the top, there is a navigation bar with links for 'Rechercher', 'JO Paris 2024', 'Politique', 'International', 'Société', 'Vox', 'Économie', 'Sport', 'Culture', 'Voyage', 'Style', 'Madame', 'Vin', and 'Se connecter'. Below the navigation bar, there is a banner for 'VENTE FLASH' (1€/mois pendant 3 mois). The main content area features a 'DOSSIER' titled 'La Chine sous toutes ses faces'. Below the title, a sub-headline reads 'De nouveaux horizons pour le patrimoine vert'. There is a large photo of the Beijing National Speed Skating Oval (Ice Ribbon) at night. At the bottom of the page, there is a 'Partager' button with links for email, Facebook, and Twitter.

Source : Site internet du Figaro, consulté le 29 juin 2024

Cette stratégie d'infiltration des médias est aussi menée par la Russie dans les pays d'Afrique francophone et documentée dans l'étude menée par Maxime Audinet sur les stratégies d'influence informationnelle russes en Afrique¹. Profitant de la précarité des écosystèmes médiatiques locaux, les opérateurs russes financent des contenus et des recrutements de journalistes relayant des positions favorables à la Russie et dénigrant la présence française dans ces pays. De même, selon le renseignement américain, la structure *African Initiative*, née sur les cendres du groupe Wagner, opère un « blanchiment » de la désinformation russe en recrutant journalistes et blogueurs pour en assurer la diffusion².

Hormis les cas de la Russie et de la Chine, la commission d'enquête s'est plus spécifiquement intéressée au rôle de la chaîne *Al Jazeera* comme vecteur d'influence du Qatar. Si le groupe *Al Jazeera* constitue indéniablement un puissant outil de diplomatie publique pour l'émirat qatari, il est moins évident d'identifier une claire stratégie d'influence négative portée par ce média. La ligne éditoriale et le contenu de ce dernier varie en effet selon les langues dans lesquelles il est diffusé. Comme l'a souligné Thibaut Brutin, adjoint au directeur général de RSF : « Il y a plusieurs *Al Jazeera*, car cette entité

¹ Maxime Audinet, *Le lion, l'ours et les hyènes. Acteurs, pratiques et récits de l'influence informationnelle russe en Afrique subsaharienne francophone*, Irsem, juillet 2021.

² Département d'État, « *Comment le Kremlin propage une désinformation mortelle en Afrique* », fiche d'information, 12 février 2024, consulté le 1^{er} juillet 2024.

émet dans différentes langues. Or les contenus produits ne sont pas les mêmes selon les antennes et les langues »¹.

En France, le débat sur les contenus diffusés par *Al Jazeera* s'est accru avec la création en décembre 2017 du média en ligne AJ+. Ce média constitue la déclinaison française d'un format existant déjà en anglais et en espagnol. AJ+ combine une ligne progressiste mettant en avant des thèmes comme l'antiracisme, les questions environnementales ou les conflits au Moyen-Orient avec des formats reprenant les codes de la modernité et des réseaux sociaux. Par rapport au format traditionnel de la chaîne *Al Jazeera*, AJ+ s'adresse à un public jeune, issu des grandes métropoles. Deux interprétations de cette stratégie ont pu être identifiées par la commission d'enquête.

D'une part, on peut estimer, à l'instar du professeur Olivier Roy, que ce média en ligne poursuit avant tout une stratégie commerciale de captation d'un public jeune à qui il fournit des contenus attractifs en leur donnant une vision plus positive de leur identité².

D'autre part, AJ+ peut être perçu comme un véritable outil d'influence négative. Une étude de la revue des médias, publiée en décembre 2020³, estime ainsi que la ligne éditoriale progressiste n'est en rien incompatible avec la vision géopolitique portée par le Qatar. **Le positionnement d'AJ+ reposera ainsi, comme pour Al Jazeera, sur la critique des gouvernements en place.** Dans le cas français, le rapport de la commission d'enquête de l'Assemblée nationale avait déjà identifié et mis en exergue **la tonalité particulièrement critique de l'émission « Rien ne va + »** envers le modèle français. De récentes vidéos s'intitulaient par exemple « Pourquoi la FFF a un problème avec les musulmans ? » (4 avril 2024), « Macron va-t-il déclencher une troisième guerre mondiale ? » (28 mars 2024), « Niger : comment l'Afrique continue de gifler Macron ! » (17 août 2023).

d) Les « contractuels de l'influence » et la nébuleuse des plateformes relais de l'influence

Outre des opérateurs clairement liés aux États compétiteurs, les opérations d'influence peuvent être menées par des acteurs non officiels qui ne rattachent pas directement à des institutions publiques. Fondations, sociétés privées ou ONG contribuent à former une « nébuleuse de l'influence ». Cette expression est notamment utilisée par Paul Charon et JeanBaptiste Jeangène Vilmer pour décrire l'ensemble des acteurs gravitant autour du régime chinois⁴.

¹ [Audition](#) du 13 juin 2024.

² [Audition du rapporteur](#), 24 juin 2024.

³ « AJ+ : derrière la modernité, le média d'influence du Qatar », *La Revue des médias*, 1^{er} décembre 2020.

⁴ Paul Charon et Jean-Baptiste Jeangène Vilmer, « Les Opérations d'influence chinoises. Un moment machiavélien », rapport de l'Institut de recherche stratégique de l'École militaire (Irsem), Paris, ministère des armées, septembre 2021 – rapport téléchargeable [ici](#).

En premier lieu, ces acteurs de l'influence regroupent des **entités du secteur privé en réalité contrôlées par des États** et réalisant pour leur compte des opérations d'influence malveillantes.

S'agissant de la Russie, cette stratégie de recours à des « *proxies* » issus du secteur privé a été largement documentée. Au sein du régime russe, des acteurs non officiels coexistent avec les institutions publiques, relevant d'une frange désinstitutionnalisée de l'État dans une logique d'« *adhocratie* ». En parallèle de l'État russe ont émergé une myriade d'entreprises de marketing numériques assurant en réalité des activités de désinformation. L'entrepreneur et mercenaire Evgueni Prigojine a ainsi pu constituer un réseau de sociétés de désinformation, autour de la célèbre *Internet Research Agency*, basée à Saint-Pétersbourg. Sans que l'on soit en mesure d'évaluer le niveau d'autonomie de ces structures par rapport au pouvoir russe, ces acteurs prolongent indéniablement la stratégie d'influence de l'État commanditaire.

Ces « *contractuels de l'influence* » ou « *prestataires d'influence ou de désinformation* » trouvent un intérêt financier direct à relayer les contenus prorusses. En Afrique, les opérateurs d'influence de l'ex-galaxie Wagner ont par exemple investi dans l'exploitation des ressources minières. À propos de son dirigeant historique, Evgueni Prigojine, Maxime Audinet rappelle que : « *C'était un acteur de nature entrepreneuriale et en fait quasiment semi-privé ; c'est pourquoi on parle « d'entrepreneurs d'influence » en utilisant un langage presque managérial ; ces acteurs ont un « business model » et cherchent à gagner du capital symbolique, financier et parfois politique* ».

Une telle méthode d'externalisation, sans pour autant duper les services chargés de la détection des opérations d'influence, complexifie l'attribution directe de ces manœuvres à un État.

Le recours à des « *contractuels de l'influence* » se diffuse à d'autres États que la Russie. La campagne de désinformation « *Olimpiya* » visant les jeux Olympiques et Paralympiques de Paris et révélée par Viginum en novembre 2023, était ainsi hébergée par des sites liés à un citoyen azerbaïdjanais, Orkhan Rzayev, dirigeant d'une entreprise de marketing digital *Mediamark Digital Agency*. Sans qu'aucun lien officiel n'ait été établi par Viginum entre Orkhan Rzayev et le régime illibéral de Bakou, l'hypothèse de l'implication de l'Azerbaïdjan demeure très probable¹.

En second lieu, au-delà de sociétés privées, la « *nébuleuse de l'influence* » rassemble également d'autres types de faux-nez civils : associations, fondations ou organisations non gouvernementales. Concernant la Chine, le rapport de l'Irsem identifie des « plateformes-relais » de l'influence chinoise comme la *China Association for International Friendly*

¹ Amaelle Guiton, « [Manipulations de l'information : Les JO de Paris visés par une campagne d'influence en ligne liée à l'Azerbaïdjan](#) », Libération, 14 novembre 2023, en ligne, consulté le 1^{er} juillet 2024.

Contact (CAIFC), la *China Association for Promotion of Chinese Culture* (CAPCC) et l'Association pour la promotion de la réunification pacifique de la Chine (APRPC). Ces entités, très liées avec le pouvoir politique et dont les membres dirigeants sont issus du PCC ou de l'armée populaire de libération, mènent des opérations d'influence, notamment en ciblant au travers d'échanges culturels les élites anglo-saxonnes.

Dans le cas de la Russie, une récente enquête de presse a dévoilé l'action de la fondation Pravfond, liée au ministère des affaires étrangères russes¹. Cette « *Fondation pour le soutien et la protection des droits des concitoyens résidant à l'étranger* » vise officiellement à défendre les Russes établis à l'étranger. Elle assure en réalité deux activités principales. D'une part, son soutien aux ressortissants russes se concentre essentiellement sur les personnes impliquées dans des affaires d'espionnage ou d'atteintes à la sécurité nationale et finance pour ce faire leurs frais de justice. D'autre part, au nom d'un objectif de « *lutte contre la russophobie et les tentatives de falsification de l'histoire* », la fondation finance des opérations d'influence en Europe. En 2023 et 2024, elle a ainsi pu soutenir l'organisation de « *conférences scientifiques* » en Serbie et en Bosnie-Herzégovine » sur le prétendu « *nazisme ukrainien* » ou abonder financièrement des sites de désinformation en ligne.

2. L'amplification numérique des opérations de manipulation de l'information

L'espace numérique constitue le **terrain privilégié de mise en œuvre des opérations de désinformation à visée d'influence**. Deux définitions, visant à caractériser les opérations de désinformation dans le domaine numérique, permettent d'appréhender ce type d'opérations.

D'une part, la notion de « *Foreign Information Manipulation and Interference* »² (FIMI) élaborée par le Service européen pour l'action extérieure (SEAE) en 2021³ présente ces actions comme un ensemble de comportements, majoritairement non illégaux, qui menacent ou ont le potentiel d'affecter négativement les valeurs et le processus politiques. Ces activités, manipulatives par dessein, sont conduites de manière coordonnée et intentionnelle par des acteurs étatiques ou non étatiques, dont des *proxies*.

D'autre part, les opérations de manipulation de l'information dans le domaine numérique ont été caractérisées par la catégorie réglementaire des **ingérences numériques étrangères** (INE), introduite par le

¹ Damien Leloup, Thomas Eydoux, Lucas Minisini et Maxime Vaudano, « [*Pravfond, la discrète caisse noire des espions russes et de leurs procès à l'étranger*](#) », Le Monde, 2 juin 2024, en ligne, consulté le 8 juillet 2024.

² Pour manipulation et ingérence étrangères de l'information.

³ SEAE, [*StratCom activity report - Strategic Communication Task Forces and Information Analysis Division*](#), 2021.

décret n° 2021-922 du 13 juillet 2021 portant création de Viginum¹. L'article R.* 1132-3 du code de la défense définit ainsi les INE comme des : « *opérations impliquant, de manière directe ou indirecte, un État étranger ou une entité non étatique étrangère, et visant à la diffusion artificielle ou automatisée, massive et délibérée, par le biais d'un service de communication au public en ligne, d'allégations ou imputations de faits manifestement inexactes ou trompeuses de nature à porter atteinte aux intérêts fondamentaux de la Nation* ».

Ces deux définitions permettent d'identifier trois caractéristiques principales des opérations de manipulation de l'information en ligne, réalisées par des entités étrangères, étatiques ou non :

- une atteinte aux intérêts de l'État visé ;
- un contenu reposant sur des informations fausses ou trompeuses ;
- une diffusion artificielle ou automatisée, massive et délibérée.

a) Une diffusion massive et inauthentique

La combinaison des nouvelles technologies de l'information et de la communication avec l'émergence des plateformes numériques permet désormais une diffusion massive et inauthentique d'informations fausses ou trompeuses.

Le fonctionnement des plateformes numériques, définies comme « *un service occupant une fonction d'intermédiaire dans l'accès aux informations, contenus, services ou bien édités ou fournis par des tiers* »², contribue activement au succès de ces opérations massives de désinformation. En effet, **au-delà d'une simple fonction d'intermédiaire, les plateformes numériques sont en mesure d'organiser et de hiérarchiser la présentation des contenus** à leurs utilisateurs. Ces mécanismes, qui rapprochent les plateformes numériques d'un rôle d'éditeur, participent de la diffusion de contenus de désinformation selon plusieurs experts auditionnés par la Commission d'enquête. À cet égard, Bernard Benhamou estime qu'il existe une « *convergence d'intérêts toxiques entre les groupes extrémistes et le modèle de fonctionnement des plateformes qui privilégie les propos polarisants, clivants, parce qu'ils sont les plus vecteurs d'audience ou vecteur d'engagement, de partage* »³.

Les opérations d'influence étrangères jouent sur ces mécanismes d'organisation des contenus endogènes aux plateformes pour accentuer la viralité de leur diffusion. Deux techniques principales peuvent être distinguées.

En premier lieu, les campagnes de manipulation de l'information peuvent recourir à des « **trolls** », soit des individus qui relaient des contenus,

¹ Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères ».

² Conseil national du numérique, *La Neutralité des plateformes*, juin 2014.

³ [Audition](#) du 4 juin 2024.

saturent des sites internet ou harcèlent d'autres utilisateurs¹. Cette dernière fonction peut être mobilisée pour réprimer tout discours dissident en interne et, en externe, cibler des discours critiques. Les groupes de trolls soutenant le régime chinois sont ainsi coutumiers de campagne de harcèlement et de dénigrement à l'encontre de personnes ou d'entités portant un discours critique sur l'action de la Chine.

Le recours aux trolls repose généralement sur la **constitution d'« usines » ou de « fermes » à trolls** directement gérées par des entités étatiques ou déléguées à des sous-traitants. C'est notamment dans ce cadre qu'interviennent des prestataires privés. **L'exemple le plus célèbre d'une telle structure demeure l'Internet Research Agency (IRA)**, dont l'existence a été publiquement révélée en 2013. Le rapport d'investigation du procureur spécial Robert Mueller sur les élections présidentielles américaine de 2016 a détaillé l'implication de cette structure dans les tentatives de manipulation du scrutin. Dotée de plusieurs centaines d'employés et pilotée par Evgueni Prigojine, **cette société aurait exposé plus de 126 millions de citoyens américains à des contenus prorusses** au travers de plus de 80 000 publications sur Facebook entre janvier 2015 et août 2017².

En second lieu, la diffusion massive de contenus faux ou trompeurs découle de **réseaux de faux comptes automatisés ou « bots »**. Ces comptes, complètement automatisés, peuvent publier des messages et contenus sans intervention humaine.

À titre d'exemple, la campagne dite RRN, révélée par Viginum en juin 2023³, a eu **massivement recours à des réseaux de comptes inauthentiques sur Facebook et X (ex-Twitter)** afin de relayer automatiquement les contenus produits par de faux comptes d'information prorusses.

La technique des *bots* présente l'avantage de demeurer rudimentaire et peu coûteuse. Par conséquent, leur détection peut s'en trouver relativement aisée. Comme l'ont indiqué les équipes de Viginum aux membres de la Commission d'enquête lors de leur visite de ses locaux, **il existe un faisceau d'indices pour détecter un faux compte**. Une photo de profil de mauvaise qualité ou générée par l'intelligence artificielle, un pseudonyme composé de chiffres et de lettres aléatoires, des contenus qui basculent soudainement dans une autre langue ou postés à la même heure chaque jour peuvent trahir l'artificialité de ces dispositifs.

¹ Jean-Baptiste Jeangène Vilmer, Alexandre Escoria, Marine Guillaume, Janaina Herrera, « [Les manipulations de l'information. Un défi pour nos démocraties](#) », rapport du Centre d'analyse, de prévision et de stratégie (Caps) du ministère de l'Europe et des affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (Irsem) du ministère des armées, Paris, août 2018.

² Colin Gérard, « [Usines à trolls](#) » russes : de l'association patriotique locale à l'entreprise globale, *La revue des médias*, 20 juin 2019.

³ Viginum, [RRN : une campagne numérique de manipulation de l'information complexe et persistante](#), Rapport technique, 13 juin 2023.

Par ces mécanismes, les auteurs de campagnes de désinformation visent avant tout à créer un effet de volume. L'utilisation massive et automatisé de faux comptes permet de créer l'illusion d'un trafic naturel important. Cette pratique d'influence correspond à la technique dite de l'« astroturfing »¹, qui consiste à simuler un mouvement spontané à des fins d'influence politique ou économique.

Auditonné par la commission d'enquête dans le cadre d'une table-ronde sur l'intelligence artificielle et la désinformation, le journaliste de l'Agence France-Presse (AFP) Grégoire Lemarchand a confirmé que ces opérations visent en premier lieu un effet de masse : « *il faut souligner que ces opérations étrangères sont, la plupart du temps, très peu sophistiquées : elles visent surtout, par un bruit de fond permanent, à saper peu à peu les fondements de notre société. La plupart des fausses informations mises en circulation ne dépassent pas le stade d'une diffusion confidentielle, mais leur répétition et leur masse finissent par produire un effet* »².

¹ En référence à une célèbre marque américaine de pelouse artificielle.
² [Audition](#) du 14 mai 2024.

Matriochka : une campagne de désinformation prorusse usurpant massivement l'identité de médias et dirigée contre les dispositifs de vérification de l'information

Viginum a détecté en septembre 2023 une campagne malveillante présentant un mode opératoire original, baptisée *Matriochka*. Son activité reposait sur la production de **faux contenus relayées vers les espaces réponses de comptes X (ex-Twitter) de médias, de personnalités et de cellules de vérifications des faits** dans un objectif de saturation de leurs capacités de traitement des demandes. Elle était opérée par des comptes russophones et semblerait liée, selon le *Washington Post*, à des sous-traitants de l'administration présidentielle russe.

Les interventions de *Matriochka* se déroulaient en deux étapes :

- en premier lieu, **un groupe de comptes, les « seeders », publiait des faux contenus sur la plateforme**. Les contenus publiés usurpaient l'identité de médias, institutions et ONG et étaient publiés en anglais, allemand, français, italien, russe et ukrainien ;

- en second lieu, **un autre groupe, les « quoters », partageait les publications diffusées en réponse à des publications de médias** ou de cellules de vérification des faits. Ces partages, intervenant 30 à 45 minutes après la publication initiale, visaient à interroger les comptes ciblés afin de leur demander une vérification de la véracité de ces contenus. Incidemment, ce mode opératoire permettait de propager largement les fausses informations contenues dans les *posts*. Ces saisines **se doublaient occasionnellement de courriers électroniques** invitant les organismes à se saisir des contenus signalés.

Environ 90 manœuvres de ce type ont été repérées par Viginum qui note, par ailleurs, qu'elles ne paraissaient pas faire l'objet d'une automatisation. Des erreurs ponctuelles ont en effet suggéré que les actions des *quoters* étaient effectuées manuellement. Les cibles **semblaient découler d'une liste préparée en avance** de chaque opération.

Chaque opération visait **entre 50 et 150 entités et individus, dont une majorité de médias**, des cellules de vérification de l'information et des personnalités travaillant dans ce domaine. Des universités, fonds d'investissement, administrations et partis politiques ont également été ciblées. En France, les médias *BFM TV*, *Le Parisien*, *Libération*, *Le Monde* et *La Montagne* ont été victimes d'usurpation d'identité.

Plus spécifiquement, une opération *Matriochka* s'est attaqué à la Banque de France en relayant une vidéo présentée comme réalisée par le Groupe Union Défense (GUD) invitant à « brûler la Banque de France ». Cette dernière était accusée de mentir sur sa solvabilité. Cette vidéo était accompagnée de faux contenus de la DGSI ou de la Banque elle-même afin d'inciter les épargnants à retirer massivement leurs liquidités.

Source : commission d'enquête d'après Viginum

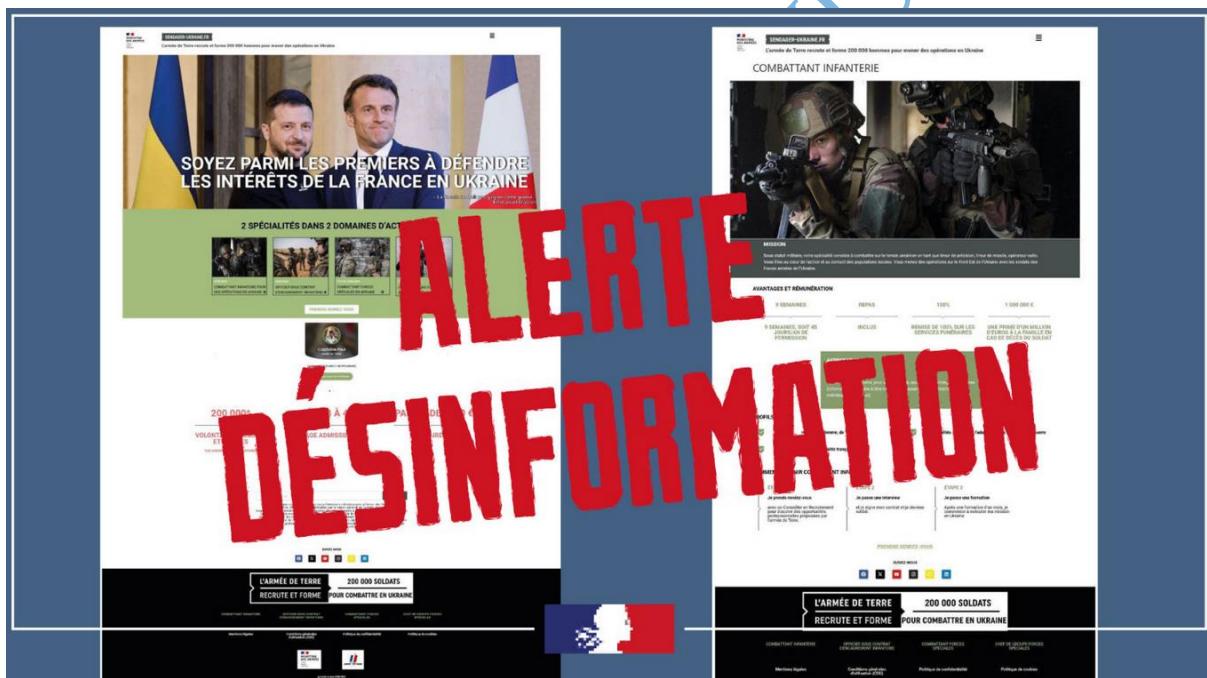
b) Les contenus et les cibles des opérations de manipulation de l'information en ligne

Les contenus propagés par les opérations de manipulation de l'information en ligne sont de nature variable. Ils peuvent **avoir été générés spécifiquement pour les besoins de l'opération où être issus d'une autre source**. S'agissant des faux contenus, trois éléments peuvent être soulignés.

Premièrement, les opérations de manipulation de l'information s'appuient sur des entreprises de falsification de contenus. Il s'agit, pour les auteurs de campagne de désinformation, **d'imiter et d'usurper des sources fiables d'information pour crédibiliser leur message.**

Il peut s'agir de sites internet d'institutions publiques. En mars 2024, le ministère des armées a dénoncé un site internet frauduleux reprenant le logo de l'armée de terre et la charte graphique des sites publics français. Appliquant une **méthode de typosquatting**, les responsables de cette action ont enregistré un nom de domaine proche (sengager-ukraine.fr) de ceux utilisés par le ministère (sengager.fr). Cette opération visait à appuyer sur la peur d'un envoi de troupes françaises en Ukraine en simulant une campagne de recrutement de 2 000 militaires contractuels.

Captures d'écran d'un faux site reprenant la charte visuelle du ministère des armées dans le cadre d'une opération de « typosquatting »



Source : ministère des armées

De manière similaire, **l'identité numérique du ministère de l'Europe et des affaires étrangères avait été usurpée en mai 2023** dans le but de diffuser l'information selon laquelle une « taxe de sécurité » en faveur de l'Ukraine serait prochainement levée.

De surcroit, les campagnes de manipulation de l'information peuvent usurper des médias existants ou se présenter comme des organes de presse. Cette imitation peut constituer un vecteur de diffusion de fausses informations. Dans le cadre de la campagne RRN, ce sont 355 noms de

domaines usurpant des médias français, européens, américains et moyen-orientaux.

La campagne RRN/*Doppelgänger* : faux médias, vraies infox

En juin 2023, la France a révélé l'existence d'une campagne numérique de manipulation de l'information liée à des entités russes, détectée en septembre 2022 par Viginum et connue sous le nom de *RRN/Doppelgänger*¹. Cette campagne s'appuyait sur **quatre modes opératoires principaux**.

Premièrement, elle reposait sur une galaxie de sites d'informations prorusses, notamment le site *RRN*, pour « *Reliable Recent News* », un média en ligne créé en mars 2022 et présentant des articles portant sur quatre thématiques : l'inefficacité des sanctions contre la Russie, la russophobie des pays occidentaux, la barbarie des forces ukrainiennes et les effets négatifs de l'accueil de réfugiés ukrainiens. L'activité de *RRN* s'appuyait, sur un plan technique, sur une plateforme de « *vérification de l'information* » dénommée « *War on Fakes* » lancée en février 2022 et abondamment relayée par la diplomatie russe. Une des caractéristiques de la campagne *RRN* est le recours fréquent à des visuels et à des caricatures critiques de l'Occident.

Deuxièmement, le réseau *RRN* a opéré une vaste opération de *typosquatting* visant à usurper l'identité de médias nationaux et de sites institutionnels européens. Viginum a ainsi identifié 355 noms de domaines usurpant l'identité de médias dans neuf États. Quatre médias français (20 Minutes, Le Figaro, Le Monde et Le Point) ont été touchés par cette manœuvre pour un total de 49 faux articles. Le site internet du ministère de l'Europe et des affaires étrangères a également été l'objet d'une tentative d'usurpation.

Troisièmement, un ensemble de sites d'information francophones comme La Virgule, Allons-y ou Notre Pays a été créé dans le but de relayer des contenus polarisants sur l'actualité française et européenne.

Quatrièmement, les contenus des sites administrés par le réseau *RRN* ont fait l'objet d'une amplification artificielle par un ensemble de comptes inauthentiques sur les plateformes *Facebook* et *Twitter/X*. Viginum a identifié plusieurs ensembles de faux comptes diffusant largement les publications de *RRN* et des sites liés.

Le groupe Meta a dénoncé cette campagne, décrite comme « *l'opération russe la plus aggressive dans sa persévérance que nous ayons vue depuis 2017* », en décembre 2022. Meta a identifié deux sociétés informatiques russes, *Social Design Agency* et *Structura National Technology*, par ailleurs prestataires d'institutions russes et dirigés par Ilya Gambachidze, un proche du Gouvernement russe. Les investigations menées par Viginum ont, par la suite, identifié deux autres « entrepreneurs d'influence » russes, Andreï Choubotchkine et Mickhaïl Tchekomasov.

Source : commission d'enquête d'après Viginum

¹ Viginum, [RRN : une campagne numérique de manipulation de l'information complexe et persistante](#), Rapport technique, juin 2023.

L'usurpation peut également être représentée dans le contenu relayé. Il est fréquent que des campagnes de manipulation diffusent des articles ou des couvertures reprenant la charte graphique ou le titre de grands titres de presse. De fausses « unes » de *Charlie Hebdo*, en relation avec les positions françaises de soutien à l'Ukraine, ont ainsi pu être réalisées et diffusées.

De même, en février 2024, **une vidéo truquée d'un journal de France 24 a été relayée par les réseaux prorusses** pour répandre la rumeur d'une tentative d'assassinat du président de la République orchestrée par le président ukrainien Volodymyr Zelensky. Cette tentative de désinformation reposait sur un hypertrucage ou « *deepfake* » du présentateur de *France 24*, réalisée grâce à la **technique de la synchronisation labiale**, qui aligne les mouvements de lèvres avec un son préenregistré. L'infox a été directement amplifiée par des publications du vice-président du Conseil de sécurité de la Fédération de Russie, Dimitri Medvedev¹.

Pour Marie-Christine Saragosse, présidente-directrice générale de France Médias Monde « *Les manipulations de l'information et les infox déferlent avec une sophistication croissante et nos médias font l'objet d'un intérêt tout particulier. Nos logos, nos émissions, nos présentateurs sont une source d'inspiration quotidienne pour les désinformateurs, qui manipulent des extraits de journaux de France 24 pour faire annoncer au présentateur, en changeant sa voix, un prétendu attentat contre le Président de la République à Kiev*

².

¹ Linh-Lan Dao, « [Vrai ou faux Comment une fausse vidéo de France 24 diffusée en Russie a lancé la rumeur d'un risque d'assassinat d'Emmanuel Macron en Ukraine](#) », France 24, 20 février 2024, en ligne, consulté le 5 juillet 2024.

² [Audition](#) du 6 juin 2024.

Fausse « une » de *Charlie hebdo* diffusée (à gauche) et hypertrucage du journaliste de France 24 Julien Fanciulli annonçant un projet d'assassinat du président Macron (à droite)



Source : RFI et France Info

Deuxièmement, les opérations de manipulation de l'information en ligne peuvent amplifier les résultats d'une action clandestine de terrain. Lors de l'affaire des étoiles de David, le réseau de désinformation RRN/Doppelgänger s'est rapidement mobilisé pour faire remonter cette actualité sur les réseaux sociaux.

Troisièmement, les outils de l'intelligence artificielle apparaissent désormais comme des accélérateurs de la production de contenus. Définie par la Cnil comme un « procédé logique et automatisé reposant généralement sur un algorithme et en mesure de réaliser des tâches bien définies », l'IA renforce le potentiel de production de faux contenus. Les outils d'IA générative à la disposition du grand public permettent déjà de réaliser, en très peu de temps, des contenus textuels et des hypertrucages de vidéos et d'images relativement crédibles et difficiles à déceler. Lors de la table ronde organisée par la commission d'enquête sur l'IA, le journaliste Thomas Huchon a pu démontrer, au travers d'une vidéo reproduisant synthétiquement la voix du président de la commission, la facilité d'utilisation de ces outils : « il nous a suffi de récupérer un extrait de deux minutes environ d'un discours et de le « donner à manger » à une intelligence artificielle pour pouvoir lui faire dire absolument tout ce que l'on veut [...]. Il est désormais possible, avec des outils numériques

extrêmement faciles d'accès, de faire dire à peu près n'importe quoi à n'importe qui »¹.

Les contenus générés par l'intelligence artificielle sont d'ores et déjà présents dans les campagnes de manipulation de l'information. À l'occasion de l'offensive russe sur Kiev au printemps 2022, les autorités russes ont diffusé sur les réseaux sociaux une vidéo hypertruquée du président ukrainien Volodymyr Zelensky appelant les troupes ukrainiennes à déposer les armes. Si l'efficacité de cette première utilisation massive de l'IA dans un contexte de guerre a été relative, elle n'en démontre pas moins les potentialités de manipulation que ces outils représentent.

Le 30 mai 2024, l'entreprise *OpenAI*, maison mère de l'instrument *ChatGPT*, a reconnu publiquement l'utilisation de ses outils par plusieurs campagnes de désinformation russes, chinoises, iraniennes et israéliennes². L'outil *ChatGPT* a notamment servi à générer des commentaires en anglais et en français, postés sur X et le forum 9GAG, dans le cadre de l'opération dite RRN/Doppelgänger.

¹ [Audition](#) du 9 avril 2024.

² [OpenAI, Disrupting deceptive uses of AI by covert influence operations](#), 30 mai 2024, consulté le 29 juin 2024.

L'utilisation de l'intelligence artificielle dans une campagne de désinformation en ligne : l'exemple de l'opération prochinoise *Spamouflage*

Depuis 2019, une opération de désinformation liée à la Chine, connue sous le nom de « *Spamouflage* »¹, a été révélée à plusieurs reprises. Le réseau *Spamouflage* repose sur des milliers de comptes inauthentiques, répartis sur une cinquantaine de plateformes et de sites.

Le mode opératoire du réseau *Spamouflage* repose sur l'usage massif de comptes inauthentiques et de bots. Dernièrement, le 29 août 2023, le groupe Meta a annoncé la suspension de plus 7 700 comptes, 954 pages et 15 groupes Facebook liés à la campagne *Spamouflage*. Le groupe estimait à un demi-million le nombre d'utilisateurs exposés à cette opération. **Le niveau de sophistication des faux comptes activés par cette campagne demeure relativement limité**, Meta ayant souligné que ces derniers publiaient à des heures fixes correspondant aux horaires de bureau chinois. L'opération **serait gérée par plusieurs services distincts disposant de moyens matériels relativement conséquents**. À cet égard, la chercheuse Maud Quessard indique que « *Ce qui ressort de nos échanges avec nos partenaires américains est que, depuis septembre 2023, la Chine se livre de plus en plus et de façon sophistiquée à des opérations de désinformation avec des méthodes et techniques qui étaient traditionnellement plutôt l'apanage de la Russie* »².

Les campagnes menées par le réseau *Spamouflage* rejoignent les codes traditionnels de la désinformation chinoise en ligne avec une forte propension à la diffusion de visuels.

Plus récemment, la société Graphika a révélé que le réseau avait désormais recours à des outils d'intelligence artificielle pour générer des contenus. De **courtes vidéos mettant en scène des avatars** relayant des éléments de discours proches de la propagande chinoise ont ainsi été détectées. Ces productions restent peu élaborées et sont issues d'outils d'IA commerciaux en libre accès.

Les contenus diffusés par *Spamouflage* suivent les priorités thématiques du régime chinois. Lors de sa première détection en 2019, le réseau relayait principalement des contenus critiques des mouvements de protestation à Hong-Kong. **La période du Covid-19 a fait évoluer ces contenus vers une promotion du modèle chinois de réponse à la pandémie** et un dénigrement des régimes occidentaux. Plus récemment *Spamouflage* a adopté une orientation centrée sur la rivalité avec les États-Unis. Les comptes liés au réseau ont **amplifié le volume de leurs publications en anglais et porté un discours plus agressif à l'égard de l'Amérique** et de ses alliés. En 2022, la société de cybersécurité Mandiant a révélé une tentative menée par le réseau d'influencer les élections américaines de mi-mandat en décourageant les électeurs de voter³.

Pour autant, l'efficacité de l'opération est discutable. Les contenus relayés par le réseau *Spamouflage* ont suscité peu de commentaires ou partages de la part des utilisateurs. **Meta estime que ce succès limité s'explique par la faible qualité des contenus postés, les opérateurs privilégiant diffuser un volume massif.**

Source : commission d'enquête d'après Meta et Graphika

¹ L'opération est également connue sous le nom de Dragonbridge, *Spamouflage Dragon* ou *Storm 1376*.

² [Audition](#) du 7 mars 2024.

³ Mandiant, [Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests, Including Midterm Elections](#), 26 octobre 2022.

La production d'un contenu original n'est cependant pas indispensable dans la conduite d'une opération d'influence informationnelle. Cette dernière peut tout à fait reposer sur un contenu préexistant, qu'elle se contente d'amplifier.

L'opération dite « *Portal Kombat* » avait ainsi **pour caractéristique de ne produire aucun contenu original** mais de relayer massivement des contenus existants, comme démontré par Viginum. Ces derniers relevaient de trois sources principales : des acteurs institutionnels russes, des agences de presse pro-Kremlin et des comptes russes ou portant un discours prorusse.

La diffusion de contenus existants permet de détecter des formes de collaborations fortuites entre les entités étatiques à l'origine à l'origine de cette désinformation. Dans son premier rapport consacré aux FIMI¹, le SEAE a identifié plusieurs occurrences de **reprise par la sphère de désinformation chinoise en ligne de narratifs et de contenus issus de la sphère russe**. Cette convergence a été soulignée par Paul Charon lors de son audition par la commission d'enquête. Dans les actions attribuées à la Chine et visant la France : « *Les contenus ne sont pas toujours très significatifs. On en trouve même parfois qui sont très prorusses et ne vont pas nécessairement dans le sens des intérêts de la Chine* »².

Outre ces contenus de propagande, d'autres types de contenus existants peuvent être relayés par les opérations d'amplification. C'est particulièrement le cas dans le cadre de **combinaison entre des opérations de manipulation de l'information et d'autres types d'ingérences**.

Le cas des opérations de piratage et de fuite (« *Hack and Leak* ») illustre cette **hybridation entre ingérence et influence**. Les opérations de piratage classiques sortent, *stricto sensu*, du champ des travaux de la commission d'enquête. Lorsqu'une opération de piratage vise la captation de données ou le sabotage d'un service ou d'une infrastructure, elle **relève du champ de la coercition et quitte celui de l'influence**. Pour autant, les **actions de *Hack and Leak***, en diffusant massivement des données volées et altérées, **poursuivent essentiellement un but d'influence**.

¹ SEAE, [« 1st EEAS Report on Foreign Information Manipulation and Interference Threats »](#), 7 février 2023.

² [Audition](#) du 6 juin 2024.

Les « *Macron Leaks* » : une opération de *Hack and Leak* en pleine campagne présidentielle

Les *Macron Leaks* désignent une campagne de manipulation de l'information, reposant sur une opération de *Hack and Leak*, réalisée dans les derniers jours de la campagne présidentielle de 2017.

Dans une première phase, relevant du domaine cyber, à partir de janvier 2017, **les équipes de campagne du candidat Emmanuel Macron ont été l'objet d'attaques répétées**, au travers de tentatives de hameçonnages. Au moins cinq collaborateurs ont vu leurs adresses mails piratées.

Dans une seconde phase, informationnelle, **les pirates ont organisé une campagne de désinformation**. Tout d'abord, des rumeurs et fausses informations ont été diffusées par l'écosystème informationnel prorusse, notamment les médias *RT* et *Sputnik*. Ensuite, les pirates ont publié, **avant le débat de l'entre-deux tours le 3 mai 2017 et après la fin de la campagne officielle le 5 mai 2017**, de faux documents nuisant à l'image du candidat. Ces documents, initialement diffusés sur des forums de discussion en ligne, ont ensuite été relayés sur Twitter. La publication des documents sur ce réseau **a été relayée par la communauté politique de l'Alt-Right américaine pro-Trump** et amplifiée par des réseaux de bots sous le mot-dièse *#MacronLeaks*.

Cette manœuvre n'a néanmoins pas prospéré. La robustesse de l'environnement informationnel français **a conduit les médias à faire preuve d'une retenue certaine dans le traitement de ces informations**. L'intérêt du public pour des milliers d'emails a largement été surestimé par les pirates qui n'avaient pas non plus anticipé que les équipes de campagne du candidat alerteraient rapidement de la survenance d'une attaque.

La France n'a jamais officiellement attribué cette manœuvre à un acteur étatique. Pour autant, le rapport Caps-Irsem relatif aux manipulations de l'information, revenant sur l'expérience des *Macron Leaks*, **identifie un faisceau d'indices incitant à penser que cette opération serait liée à une influence russe**¹. De même, le rapport de la commission d'enquête de l'Assemblée nationale relatives aux ingérences de puissances étrangères en France attribue très clairement à la Russie cette campagne de désinformation.

Source : commission d'enquête d'après le rapport Caps-Irsem

Au bilan, les opérations de manipulation de l'information en ligne, au-delà de leurs spécificités techniques ou de leurs contenus et cibles, présentent de fortes similarités. Parmi ces points de convergence **figure le faible coût de ces opérations**. S'il est difficile de fournir une évaluation moyenne précise d'une opération type, le service Viginum estime qu'il correspond peu ou prou à celui d'une campagne de publicité en ligne. Le

¹ Jean-Baptiste Jeangène Vilmer, Alexandre Escoria, Marine Guillaume, Janaina Herrera, « [Les manipulations de l'information. Un défi pour nos démocraties](#) », rapport du Centre d'analyse, de prévision et de stratégie (Caps) du ministère de l'Europe et des affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (Irsem) du ministère des armées, Paris, août 2018.

budget de *Pravfond*, fondation faux-nez du ministère des affaires étrangères russes finançant des opérations de désinformation en Europe, **était ainsi évalué par Le Monde à 3 à 4 millions d'euros par an**. Pour un État, quel que soit sa taille, ces opérations sont donc relativement bon marché et contribuent à faire de ces manœuvres **des armes du faible au fort permettant de frapper des États disposant de largement plus de moyens**.

B. LES AUTRES TYPES D'OPÉRATIONS D'INFLUENCE

1. Les opérations visant l'enseignement supérieur et la recherche

Comme indiqué *supra*, le secteur de l'enseignement supérieur et de la recherche est **particulièrement exposé aux opérations d'influence étrangères**. Un riche panorama ayant d'ores et déjà été établi par la mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences¹, la commission d'enquête limitera ici à en rappeler les points saillants.

Les stratégies des puissances étrangères dans le milieu universitaire poursuivent deux principaux objectifs :

- d'une part, **défendre et promouvoir la réputation d'un État au sein des universités**. Il s'agit pour ces États d'assurer la promotion de valeurs alternatives au modèle de société porté par 'les pays occidentaux, au besoin par une instrumentalisation des sciences humaines et sociales ;

- d'autre part, **opérer une captation de données scientifiques sensibles pour les intérêts de la Nation ou protégées par la propriété intellectuelle**. Cette captation permet d'obtenir des avantages immédiats sur les plans techniques et économiques mais renforce également l'influence académique de l'État à l'origine de cette intrusion.

Pour le rapporteur de la mission d'information du Sénat, André Gattolin, l'exemple des opérations d'influence dans le domaine universitaire permet de garder à l'esprit qu'en matière d'influence, **il importe de s'écartier d'un « prisme numérique et technologique » et de considérer la persistance de réseaux d'influence physiques, sur le terrain**².

2. La capture des élites : idiots utiles et trahison des clercs

Au regard des stratégies de capture des élites, plusieurs modalités peuvent être distinguées. Ces opérations peuvent poursuivre un **objectif d'influence directe sur des décideurs publics** ou, plus indirectement, utiliser

¹ [*Rapport d'information n° 873 \(2020-2021\)*](#), fait par André Gattolin au nom de la mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences, déposé le 29 septembre 2021.

² Audition par le rapporteur le 6 mai 2024.

les élites politiques ou économiques comme relais d'influence auprès d'autres interlocuteurs et de l'opinion publique.

Premièrement, les États étrangers peuvent avoir recours aux services de représentants d'intérêts ou de lobbyistes pour porter un discours d'influence auprès des responsables publics.

Deuxièmement, **le financement des partis politiques constitue un levier d'influence efficace pour des États étrangers**, notamment s'il permet à des personnalités publiques d'accéder à des fonctions électives.

Troisièmement, **des actions de corruption** permettent à des puissances étrangères de capter des relais d'influence moyennant finances.

À titre d'illustration, révélé en décembre 2022, le « *Qatargate* » a concerné plusieurs eurodéputés dont une vice-présidente du Parlement européen ainsi que des responsables d'ONG. Ces derniers auraient reçu d'importantes sommes d'argent en liquide dont les autorités belges soupçonnent qu'elles aient été versées par le Qatar et le Maroc en échange de prise de position favorables à l'Émirat.

Au-delà de cas de corruption aussi poussés, il existe toute une palette de pratiques (cadeaux, invitations, mobilités professionnelles...) **entrant dans une zone grise des obligations déontologiques des élus**. S'agissant du Parlement français Nicolas Tenzer, président du CERAP considère ainsi qu'« *on ne peut pas aborder, soyons parfaitement directs, la question de l'influence de puissances hostiles sinon ennemis, comme la Russie ou la Chine, sans parler de corruption* »¹.

Quatrièmement, **le phénomène des « idiots utiles »**² demeure d'actualité. Par opportunisme ou par conviction, des journalistes, élus ou hauts fonctionnaires peuvent reprendre des éléments de narratifs portés par des puissances étrangères. Le député européen Arnaud Danjean a ainsi souligné qu'une grande partie des membres du Parlement européen relayant des discours prorusses étaient sincèrement convaincus par ces éléments. À cet égard, la commission d'enquête renvoie vers les travaux de la commission d'enquête de l'Assemblée nationale sur les ingérences dans la vie politique française³ qui relève, de l'extrême-gauche à l'extrême-droite de l'échiquier politique, une adhésion aux thèses du Kremlin revendiquée par des figures de premier plan. En outre, au cours des auditions, les membres de

¹ [Audition](#) du 29 février 2024.

² En référence à une citation apocryphe de Lénine désignant les intellectuels occidentaux favorables au régime soviétique.

³ [Rapport n°1311 \(seizième législature\)](#) fait par Constance Le Grip au nom de la commission d'enquête de l'Assemblée nationale relative aux ingérences politiques, économiques et financières de puissances étrangères - États, organisations, entreprises, groupes d'intérêts, personnes privées - visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français déposé le 1^{er} juin 2023, Tome I.

la commission d'enquête se sont interrogés sur les motivations des prises de position d'un ancien Premier ministre en faveur de la Chine.

3. Le contrôle et l'instrumentalisation des diasporas et des communautés religieuses

En premier lieu, il importe de distinguer les actions d'entités étrangères sur leurs ressortissants présents en France selon leurs finalités. Seule une partie des activités d'ingérence portant sur des membres de la diaspora relève en effet d'un objectif d'influence. L'autre part de ces actions vise principalement à assurer un contrôle de l'État étranger sur une population qu'il considère comme ressortissant de sa souveraineté.

L'exemple de la diaspora chinoise est topique de cette logique, comme cela a été exposé *supra* (voir II). Dès lors que la diaspora est entendue comme une menace, des mesures de contrôle peuvent être envisagées, **dont la maîtrise des médias de la langue de la diaspora ou des actions coercitives assurées par les consulats et les ambassades**. Une fois placée sous contrôle, la diaspora peut être mobilisée dans un but d'influence, notamment par des actions d'ingérence dans la vie politique locale. À cet égard Paul Charon évoque : « *plusieurs cas, y compris en France, d'opérations menées par la police chinoise, donc par le ministère de la sécurité publique, à l'encontre de citoyens chinois ou de citoyens français d'origine chinoise* ». Il en résulte que « *la diaspora, qui est donc une menace, devient un vecteur d'influence une fois qu'elle est sous contrôle* »¹.

En second lieu, les **communautés religieuses apparaissent également comme un vecteur d'influence**. La commission d'enquête s'est interrogée sur les stratégies d'influence déployées par des États du monde musulman vers les communautés musulmanes des pays européens. Cette crainte d'une influence étrangère sur l'islam français a été portée au plus haut de l'État, par le Président de la République dans son discours des Mureaux du 2 octobre 2020 où il s'engageait à libérer « *l'islam en France des influences étrangères. Sur ce sujet, nous allons le faire de deux manières, parce qu'il y a deux types d'influences. Il y a une influence qui est visible, qui est assumée, et il y a une influence qui est parfois plus profonde et dangereuse, mais qui est moins visible et moins assumée* »². Cette problématique est une préoccupation ancienne du Sénat, comme l'illustre le rapport des sénateurs Nathalie Goulet et André Reichardt au nom de la mission d'information sur l'organisation, la place et le financement de l'Islam en France et de ses lieux de culte³.

¹ [Audition du 6 juin 2024](#).

² [Discours du Président de la République sur le thème de la lutte contre les séparatismes](#), 2 octobre 2020.

³ [Rapport n° 757 \(2015-2016\) fait par Nathalie Goulet et André Reichardt au nom de la mission d'information sur l'organisation, la place et le financement de l'Islam en France et de ses lieux de culte, déposé le 5 juillet 2016](#).

La communauté académique française est quant à elle divisée sur la question des influences étrangères islamistes.

Pour le professeur Bernard Rougier, auditionné par le rapporteur, **le Qatar soutiendrait idéologiquement le mouvement des Frères musulmans par des programmes de théologie et des actions de lobbying** auprès des institutions européennes, tout en restant prudent sur l'ampleur de ces actions¹.

Selon le professeur Olivier Roy, auditionné également, l'Arabie Saoudite aurait « *coupé les ponts* » avec le salafisme européen en adoptant une politique de tarissement des financements. De même, pour ce chercheur, **le positionnement idéologique du Qatar en soutien aux Frères musulmans aurait été mis en sommeil suite aux tensions géopolitiques** ayant traversé le Golfe².

En tout état de cause, **le modèle de la « *croyance rémunérée* »**, identifié par Frédéric Charillon pour décrire l'influence déployée par les pays musulmans à l'égard de leurs coreligionnaires, présente des limites en termes d'efficacité. Frédéric Charillon souligne ainsi que : « *L'influence ainsi déployée est clivante par définition puisqu'elle est identitaire. Elle sous-traite des stratégies à des acteurs qui ont leur propre agenda. En liant croyance et argent, elle déclenche une dynamique de surenchère, qui a ses fragilités* »³.

De plus, comme le rappelle Olivier Roy, **les mouvements fréristes et salafistes en Europe sont désormais endogènes à nos sociétés** et relèveraient, non pas d'une influence extérieure, mais plutôt d'une problématique interne aux États européens. Ce dernier constat n'écarte en rien la nécessité de porter une attention particulière au phénomène du communautarisme, mais semble sortir cette problématique du champ des influences étrangères.

En tout état de cause, le phénomène des influences étrangères sur le religieux devrait continuer d'être suivi par les services de l'État. La mission, confiée par le ministre de l'intérieur et des Outre-mer et le ministre de l'Europe et des affaires étrangères à l'Ambassadeur François Gouyette et au Préfet Pascal Courtade, d'évaluation de l'islamisme politique et de la mouvance des Frères musulmans **devrait permettre de prolonger cette réflexion et d'affiner le constat de la commission d'enquête**.

Les tentatives d'influence des communautés religieuses depuis l'étranger **sont plus évidentes s'agissant de deux États particuliers : le Maroc et la Turquie**. Néanmoins, davantage qu'une application du « *modèle golifique* » décrit par Frédéric Charillon et de la poursuite d'objectifs prosélytes de conquête des cœurs et des esprits, **les stratégies marocaines et turques s'inscrivent davantage dans une optique de contrôle de leurs diasporas**.

¹ *Audition du rapporteur, 16 mai 2024.*

² *Audition par le rapporteur le 24 juin 2024.*

³ *Frédéric Charillon, Guerres d'influence, « Chapitre 6. Rémunérer la croyance, ou le modèle golifique », Odile Jacob, 2022.*

Selon le comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR), **plusieurs structures religieuses turcophones sont susceptibles de relayer l'influence du régime turc en Europe**¹. Il s'agit notamment de la confédération islamique *Millî Görüş*, présente en France au travers de plusieurs associations, mosquées, centres culturels et écoles privées hors contrat. La confédération est liée avec le parti islamo-conservateur (AKP), au pouvoir en Turquie. En outre, l'organisation *Ditib* (Union turco-islamique des affaires religieuses)², rattachée à l'Agence des affaires religieuses de Turquie, gère des mosquées et des centres culturels en Allemagne et dans d'autres pays européens. **Ces structures sont susceptibles de mobiliser la diaspora turque en faveur du régime Erdogan, notamment en période électorale.**

En particulier, l'influence des pays d'origine, essentiellement l'Algérie, le Maroc et la Turquie, sur les diasporas en France, au travers de l'organisation du culte musulman, avait déjà été soulignée dans le rapport de la mission d'information sénatoriale précitée. Le rapport identifiait six principaux leviers d'exercice de cette influence :

- par les rapports avec les mosquées implantées sur le territoire ;
- dans la répartition tripartite et essentiellement nationale des trois principales fédérations musulmanes de France ;
- dans la composition et la gouvernance du Conseil français du culte musulman ;
- dans l'organisation de la filière hallal ;
- dans la formation des imams, objet d'un oligopole entre l'Algérie, le Maroc et la Turquie ;
- dans la désignation des imams exerçant en France.

Sur ce dernier point, on peut souligner que la fin des imams détachés, annoncée par le président de la République et le ministre de l'intérieur, ne règle pas la question des influences étrangères susceptibles de peser sur la formation et la désignation des imams.

Dans son rapport annuel 2022-2023³, la délégation parlementaire au renseignement a notamment pointé la persistance à cet égard d'une activité marocaine et d'une activité algérienne en lien avec la Grande Mosquée de Paris, tout en relevant que la loi du 24 août 2021 confortant les principes de la

¹ *Audition de M. Étienne Apaire, secrétaire général du comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR) le 4 avril 2024 (huis clos).*

² *Pour Diyanet İşleri Türk İslam Birliği.*

³ *Rapport public n° 1454 (Assemblée nationale seizième législature)/ n° 810 – (Sénat 2022-2023)* fait au nom de la délégation parlementaire au renseignement, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023, déposé le 29 juin 2023.

République¹ avait conféré à l'administration de nouveaux moyens de contrôle et d'entrave (voir *Deuxième partie, III, E*).

Les auditions de chercheurs et des services de l'État menées par la commission d'enquête ou par le rapporteur n'ont pas permis d'identifier d'éléments nouveaux par rapport à ces travaux.

Pour autant, malgré le renforcement de notre arsenal juridique de contrôle, le risque d'opérations d'influence visant la communauté musulmane française par l'intermédiaire de canaux plus complexes ne doit pas être écarté. La commission d'enquête estime nécessaire que les services de renseignement et les services chargés de la veille des opérations d'influence étrangères malveillantes maintiennent un niveau de vigilance élevé quant à une potentielle instrumentalisation des communautés religieuses. Il conviendra également de remédier à certaines lacunes persistantes de nos moyens de contrôle issus de la loi confortant les principes de la République (voir *Troisième partie, III, D*).

.....

4. Les opérations d'influence dans le domaine économique

Identifier et caractériser les opérations d'influence dans le champ économique paraît complexe au regard de l'objet de la commission d'enquête. Il paraît nécessaire de **distinguer les actions de puissances étrangères dans le domaine économique qui poursuivent un objectif de compétition économique et celles qui visent un objectif d'influence**.

L'action des services du ministère de l'économie et des finances se concentre sur les vulnérabilités de secteurs de l'économie jugés stratégiques. Il s'agit d'une **approche fondée sur la sécurité économique davantage que sur la prévention des influences malveillantes**. Les dispositifs de veille et de traitement des menaces sur les entreprises stratégiques françaises, qui sont exposées dans la seconde partie du présent rapport, **n'englobent pas les menaces relevant de l'influence**. Ils se concentrent notamment sur les opérations de nature capitalistiques et la captation des données sensibles.

Pour autant, il apparaît que des investissements économiques peuvent être placés au service d'une politique d'influence. S'agissant de la Chine, **l'utilisation du levier économique et commercial pour atteindre des objectifs politiques est largement documenté**. Le poids des investissements chinois dans certains États et la taille du marché intérieur chinois peuvent être notamment utilisés pour inciter États et entreprises à reprendre des éléments de discours de la propagande du PCC.

Concernant d'autres États, **il est moins évident d'identifier si des investissements visent ou non un but d'influence**. La commission d'enquête

¹ Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République.

s'est ainsi interrogée sur les objectifs poursuivis par les opérations économiques réalisées ou annoncées par des États du Golfe en France. Spécialiste de l'islam, le Professeur Olivier Roy estime que **les financements apportés par le Qatar dans certains secteurs de l'économie, comme le sport, relèvent « plus du hobby que du lobby »**¹. De même Joffrey Célestin-Urbain, chef du Service de l'information stratégique et de la sécurité économiques (Sisse), considère que **ce type d'investissements s'inscrit dans une simple logique de compétition économique** : « *Les fonds des pays du Golfe sont largement attirés en France, dans de nombreux secteurs, qui ne sont pas tous stratégiques. Nous ne pouvons pas nous passer des fonds étrangers : l'ampleur des besoins de financement de la tech française et de la tech européenne est telle, par rapport aux capacités de financement endogènes de l'Europe, que l'on ne peut pas faire autrement, à moins d'envoyer des licornes et des scale-up françaises au casse-pipe* »².

La portée des investissements étrangers en termes d'influence constitue un point sur lequel les travaux de la commission d'enquête n'ont pas permis de progresser.

Dans la même logique, les actions de « *lawfare* », soit l'utilisation de l'arme normative, menées par des États étrangers à l'encontre d'entreprises ou de ressortissants français ne relèvent pas systématiquement du domaine de l'influence. Le *lawfare* constitue l'utilisation du droit et des procédures judiciaires à des fins stratégiques par une entité étatique.

Cette méthode d'ingérence économique est particulièrement pratiquée par les États-Unis. Ces derniers **s'appuient sur l'extraterritorialité de leur droit, en particulier le Foreign Corrupt Practices Act (FCPA)**³ et **l'International Traffic in Arms Regulations (ITAR)**⁴, pour capter des données confidentielles. Cette instrumentalisation du droit permet aux autorités américaines de contraindre des entreprises étrangères, sous la menace d'amendes considérables, de coopérer et de fournir des informations stratégiques. Ces méthodes **poursuivent en premier lieu un objectif de capture de secrets industriels**, dans une logique de compétition économique aggressive et non d'influence sur les acteurs économiques français.

Pour autant, d'autres formes de *lawfare* peuvent davantage se rattacher à des opérations d'influence. Il s'agit tout particulièrement de **la pratique des « procès baillons » par lesquels des puissances étrangères ou leurs représentants peuvent agir pour contraindre au silence des discours critiques**. Ces procédures poursuivent un double objectif de communication à l'égard du public (faire savoir qu'une plainte a été déposée) et **d'épuisement des ressources financières de la personne ou de l'entité visée** (en les incitant *in fine* à l'autocensure).

¹ *Audition par le rapport le 24 juin 2024.*

² *Audition* du 8 avril 2024.

³ *Pour la loi relative à la corruption d'agents publics étrangers.*

⁴ *Pour la réglementation du trafic d'armes au niveau international.*

À titre d'exemple, à la suite de la publication du rapport Caps-Irsem sur les manipulations de l'information, **la chaîne RT France a engagé en décembre 2018 une procédure en diffamation** contre Jean-Baptiste Jeangène Vilmer, auteur du rapport et les directeurs de publication des sites sur lesquels le rapport a été publié. Ce dernier a été visé par une seconde procédure pour une série de publications sur Twitter défendant le rapport face aux critiques de RT. **Les deux plaintes ont échoué, permettant, par retour de bâton, au chercheur de contre-attaquer** en dénonçant les méthodes d'intimidation de RT et de démontrer l'incontestable dépendance de ce média à l'égard du Kremlin¹.

DOCUMENT PROVISOIRE

¹ Communiqué de Jean-Baptiste Jeangène Vilmer, [« Affaire Jean-Baptiste Jeangène Vilmer / RT France : RT France perd son procès au tribunal et fait appel »](#), Irsem, 15 juin 2022.

DEUXIÈME PARTIE : UN DISPOSITIF DE PROTECTION ÉTOFFÉ MAIS À GÉOMÉTRIE VARIABLE, SANS STRATÉGIE D'ENSEMBLE

I. DÉTECTION ET CARACTÉRISATION : UN DISPOSITIF RESSERRÉ AUTOUR DES MINISTÈRES RÉGALIENS

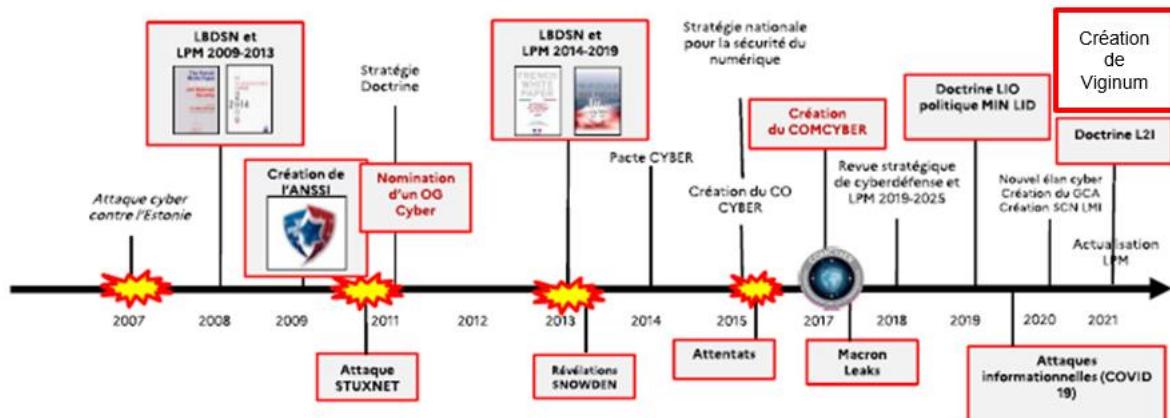
A. *UN PROCESSUS EMPIRIQUE D'ÉLABORATION DES STRATÉGIES SUCCESSIVES DE LUTTE INFORMATIQUE DÉFENSIVE, OFFENSIVE ET INFORMATIONNELLE*

Au vu des typologies de menaces présentées dans la partie précédente, on peut chronologiquement dater la survenance des événements qui ont conduit le gouvernement à mettre en œuvre les politiques publiques successives pour y répondre :

- la création de l'Agence nationale de sécurité des systèmes d'information (Anssi) en 2009, à la suite de l'attaque cyber russe de 2007 qui a paralysé pendant 48 heures l'État estonien et de la loi de programmation militaire 2009-2013¹, la première à définir des obligations de cybersécurité pour les opérateurs d'importance vitale (OIV) ;
- la création du commandement de la cyberdéfense (Comcyber) de l'état-major des armées en 2017 à la suite de multiples événements liés à la cybersécurité des armées et de la propagation du terrorisme et des idéologies islamistes via les réseaux sociaux en provenance du Levant ;
- enfin, suivant la frise chronologique ci-après, la création du service de vigilance et de détection des ingérences numériques étrangères (Viginum) en 2021 suite à l'affaire des « *Macron leaks* » et aux opérations de désinformation liées à la pandémie de Covid-19.

¹ Loi n° 2009-928 du 29 juillet 2009 relative à la programmation militaire pour les années 2009 à 2014 et portant diverses dispositions concernant la défense

Chronologie des établissements en charge de la cybersécurité, de la cyberdéfense et des ingérences numériques étrangères



Source : ministère des armées, Comcyber

La création d'acteurs dédiés (Anssi et Comcyber) a entraîné, suivant un processus logique mais empirique, l'élaboration de stratégies ou de doctrines d'emploi. Ainsi en a-t-il été de la publication d'une stratégie nationale pour la sécurité du numérique en 2015, soit six ans après la création de l'Anssi. Ont également suivies en 2018 une revue stratégique de cyberdéfense des armées puis, en 2019, une doctrine de lutte informatique offensive (LIO) et en 2021 une doctrine de lutte informatique informationnelle (L2I) à l'usage spécifique du Comcyber.

Dans le prolongement de cette chronologie, on peut donc anticiper que dans la seconde étape de la création du Viginum, une stratégie nationale de lutte contre les manipulations de l'information provenant de l'étranger soit élaborée et rendu publique dans un objectif de participation et de résilience de la société civile. Cette perspective fait l'objet d'une recommandation de la commission d'enquête (voir *Troisième partie, I*).

La visite sur place de Viginum effectué par la commission d'enquête a permis de préciser le périmètre d'activité de ce service à compétence nationale et d'en mesurer également les limites et les recommandations de la commission qui seront exposées dans les sections suivantes.

B. UN TRAVAIL DE DÉTECTION ET DE RIPOSTE DES OPÉRATIONS REPOSANT SUR LA MOBILISATION DE PLUSIEURS ACTEURS

1. Viginum, protecteur du débat public numérique national

Pour mémoire, le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) a été institué par un décret du 13

juillet 2021¹, est un service à compétence nationale rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN) (voir *Première partie, IV*)

Ce décret confie spécifiquement à Viginum la mission de **déetecter et caractériser « en source ouverte », c'est-à-dire en analysant les contenus accessibles publiquement sur les plateformes en ligne, les ingérences numériques étrangères**, notamment lorsque celles-ci sont de nature à altérer l'information des citoyens pendant les périodes électorales.

Pour mener à bien cette mission, le pouvoir réglementaire a autorisé Viginum à **mettre en œuvre un traitement informatisé et automatisé de données à caractère personnel**, selon des modalités encadrées². Celui-ci est cependant encadré, et ne peut être effectué qu'aux seules fins de détecter et de caractériser des ingérences numériques étrangères, notamment lorsque ces opérations sont de nature à altérer l'information des citoyens pendant les périodes électorales. Ce traitement repose sur la collecte et l'exploitation des contenus publiquement accessibles aux utilisateurs des plateformes en ligne dont l'activité sur le territoire français dépasse un seuil de cinq millions de visiteurs uniques par mois.

Il est par ailleurs à noter que l'activité de Viginum, en particulier au titre de ses prérogatives de traitement automatisé de données, est suivie par un **comité éthique et scientifique**, qui peut adresser au chef du service toute recommandation sur les conditions d'exercice des missions du service.

Viginum constitue ainsi le **seul service de l'État qui dispose à la fois d'une mission explicite en matière de veille/détection/caractérisation, en sources ouvertes, des ingérences numériques étrangères et d'une autorisation de collecte et d'analyse des données à caractère personnel**.

À cet égard, il convient de relever que **Viginum n'est pas un service de renseignement, de telle sorte qu'il ne saurait « attribuer » une opération d'ingérence à un État déterminé** – tout au plus, le service peut caractériser une ingérence émanant d'acteurs « prorusses », « prochinois », pro-Azerbaïdjan » etc.

Viginum n'est pas non plus un « ministère de la vérité » - pour reprendre le célèbre concept de George Orwell - en ce qu'il n'entend ni démythifier (*debunking*), ni de vérifier les faits (*fact-checking*) relayés par les contenus diffusés dans le cadre de l'opération d'INE, et encore moins de produire un contre-narratif : de telles missions, en effet, relèvent soit des médias, soit de l'autorité politique dans le cadre d'une dénonciation publique, mais en aucun cas d'un service administratif. **Sa mission se limite à la**

¹ Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères ».

² Décret n° 2021-1587 du 7 décembre 2021 portant autorisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères.

caractérisation de l'INE, qui procède de la détection de comportements inauthentiques sur les plateformes (utilisation de *bots*, de faux comptes *etc.*) visant à diffuser de façon massive et artificielle des contenus participant d'une volonté d'influence malveillante des citoyens français menée par un acteur étranger.

Il peut recevoir des informations, à cette fin, avec les autres acteurs susceptibles de détecter des comportements sur les réseaux sociaux représentant une menace potentielle, en particulier la direction générale de la sécurité intérieure (DGSI) ou encore le Comcyber.

Ces caractéristiques particulières permettent de positionner Viginum comme un interlocuteur crédible des médias, qui relaient largement ses analyses techniques publiées sous forme de rapports. Ont notamment récemment donné lieu à une publication les rapports techniques relatifs aux opérations prorusses *RRN/Doppelganger*¹, *Portal Kombat*², et *Matriochka*³, ainsi qu'une fiche technique sur manœuvres informationnelles d'origine azerbaïdjanaise ciblent la France dans le contexte des émeutes en Nouvelle-Calédonie⁴.

Pour mener ce travail de détection, l'activité de Viginum est structurée autour d'« opérations », conduite par un groupe d'agents travaillant sur un même plateau technique. Ces opérations sont de trois types :

- les opérations permanentes de veille sur un secteur déterminé, soit géographique (acteurs prorusses, acteurs asiatiques...), soit thématique (intérêts économiques, industriels et scientifiques français) ;
- les opérations liées aux élections ;
- les opérations liées à des crises ou à des évènements particuliers.

¹ Viginum, [RRN, une campagne numérique de manipulation de l'information complexe et persistante](#), Rapport technique, juin 2023.

² Viginum, [Portal Kombat, un réseau structuré et coordonné de propagande prorusse](#), rapport technique, février 2024.

³ Viginum, [Matriochka, une campagne prorusse ciblant les médias et la communauté des fact-checkers](#), rapport technique, juin 2024.

⁴ Viginum, [« Sur X et Facebook, plusieurs manœuvres informationnelles d'origine azerbaïdjanaise ciblent la France dans le contexte des émeutes en Nouvelle-Calédonie »](#), Fiche technique, 17 mai 2024.

Les opérations de Viginum en cours (juin 2024)

Type d'opération	Lancement	Thématique
Permanente	Depuis 2022	Sphères arabophone, turcophone et persanophone
Permanente	Depuis 2023	Europe de l'Est
Permanente	Depuis 2022	Mouvance conservatrice anglophone
Élections	Depuis 2023	Élections au Parlement européen
Évènement	Depuis 2023	Jeux Olympiques et Paralympiques de 2024
Évènement	Depuis 2022	Tir de missile M51
Permanente	Depuis 2022	Intérêts économiques industriels et scientifiques français
Permanente	Depuis 2022	Asie

Source : Viginum, d'après les réponses au questionnaire du rapporteur

Pour conduire ces actions, le service devrait être doté de **58 équivalents temps plein (ETP) d'ici à la fin de l'année 2024**, dont une quarantaine affectée aux opérations. Les effectifs ont ainsi connu une hausse marquée depuis 2021, année de création du service, où ils s'élevaient à 40 ETP.

Le budget du service, hors dépenses de personnel (dépenses de titre 2) est de 3,1 millions d'euros en 2024. La masse salariale (dépenses de titre 2) liée au service, qui ne fait pas l'objet d'une ligne budgétaire spécifique dans la mesure où celle-ci est incluse dans l'enveloppe du SGDSN) peut-être estimée à environ 4,2 millions d'euros en 2024. **Ainsi, le budget global de Viginum est d'environ 7,3 millions d'euros.**

À la demande du rapporteur, Viginum a été en mesure de fournir une estimation des moyens nécessaires à la caractérisation d'une opération sophistiquée, de type *RRN* ou *Portal Kombat*. D'après les réponses de ce service :

- la mobilisation minimale durant 30 jours de six agents (deux analystes, un *data scientist*, un chargé de mission coordination, une conseillère juridique et un cadre) à raison d'une journée à 2 000 euros, soit 60 000 euros pour les moyens humains ;

- l'utilisation de moyens techniques spécifiques (infrastructure, logiciels et applicatifs) sur la même durée de temps, soit 60 000 à 80 000 euros.

Ainsi, hors moyens généraux (alimentation, électricité, coûts de fonctionnement de la structure), la détection et la caractérisation d'une seule

INE sophistiquée pourrait représenter un coût approximatif entre 120 000 et 140 000 euros.

Ce coût doit néanmoins être rapporté au fait que, comme cela sera rappelé infra (voir II), la détection d'une opération d'ingérence impose mécaniquement des coûts en retour à l'adversaire, qui est ainsi contraint de changer son mode opératoire s'il entend mener de nouvelles opérations.

2. La direction de la communication et de la presse : bras armé du Quai d'Orsay pour la veille stratégique

Tandis que l'activité de détection et de caractérisation de Viginum s'attache à protéger le débat public numérique national, il appartient au ministère de l'Europe et des affaires étrangères d'assurer la fonction de veille quant aux opérations qui viseraient à porter atteinte à l'image de la France à l'étranger.

En son sein, cette mission relève de la direction de la communication et de la presse (DCP). Par un arrêté du 9 août 2022¹ entré en vigueur le 1^{er} septembre 2022, celle-ci s'est en effet dotée, d'une sous-direction « veille et stratégie », qui est active depuis novembre 2022.

Dans le détail, celle-ci est chargée :

- de l'analyse du champ médiatique français et du champ informationnel international ;
- des stratégies de riposte aux attaques informationnelles et de la coordination des actions de communication stratégique.

Par ailleurs, elle accompagne les directions internes et le réseau diplomatique aux enjeux de lutte contre la désinformation et participe au travail interministériel en matière de lutte contre les manipulations de l'information.

Pour mener ces missions, la DCP sur 22 ETP, total appelé à être portée prochainement à 27 ETP selon les éléments transmis à la commission d'enquête par le ministère (sur les 128 ETP que compte la direction), et sur un budget de 2,6 millions d'euros, (sur 7,5 millions d'euros pour l'ensemble de la DCP).

La DCP s'efforce de développer une culture de la veille en sources ouvertes proche de celle de Viginum. Comme l'a indiqué son directeur Christophe Lemoine lors de son audition devant la commission d'enquête : « *la veille traditionnelle du quai d'Orsay s'est transformée, passant des revues de presse à un processus plus dynamique et attentif aux réseaux sociaux. Les équipes disposent à présent d'outils pour cerner les tendances en termes de narratifs en*

¹ Arrêté du 9 août 2022 modifiant l'arrêté du 28 décembre 2012 relatif à l'organisation de l'administration centrale du ministère des affaires étrangères.

circulation. (...) Il importe de disposer d'une vision globale des réseaux sociaux, où chacun, du fait des algorithmes en place, est incité à consulter tel contenu plutôt que tel autre, en fonction de ce à quoi il s'intéresse déjà »¹.

Il convient cependant de noter que, contrairement à Viginum, aucun cadre juridique ne permet à la DCP de procéder à un traitement automatisé de données à caractère personnel.

3. Les armées : une veille constante des menaces informationnelles par le Comcyber et la Dicod

Dans le champ des armées, deux acteurs se sont dotés de capacités de veille et d'alerte.

Le travail de détection d'une opération de lutte informationnelle visant l'action des forces françaises sur un théâtre extérieur relève du commandement de la cyberdéfense de l'état-major des armées (Comcyber).

Le Comcyber connaît une hausse importante de ses moyens. Aussi, le nombre de cybercombattants est passé de 3 000 personnels en 2019 à 4 600 en 2024 et a atteindrait 5 600 en 2030 selon la trajectoire prévue par la loi de programmation militaire 2024-2030². Son budget est d'environ 40 millions d'euros en 2024, et doit être porté à 80 millions d'euros d'ici à 2028.

La capacité de veille/alerte du Comcyber est constituée de plateaux chargés de la veille d'infosphères d'intérêt opérationnel sur leur zone géographique d'intérêt. D'après les informations communiquées à la commission d'enquête par l'état-major des armées, ces plateaux émettent une à deux alertes quotidiennes.

Cette mission a été décrite devant la commission d'enquête par le général de division Aymeric Bonnemaison, commandant de la cyberdéfense : « *Concrètement, nous faisons de la veille-alerte pour détecter les attaques informationnelles contre nos armées et les opérations qu'elles mènent. Cela peut sembler simple, mais c'est comme surveiller un océan : nous devons détecter toute opération et déterminer par sa caractérisation si elle est inauthentique et coordonnée par un État, et pas seulement l'expression d'un particulier.* »³.

Sur le champ du travail de veille effectué par le Comcyber, le général Bonnemaison précise que « *la première mission, ce sont les théâtres d'opération, mais nous sommes obligés d'élargir le cercle et cela concerne aussi les pays voisins et les grandes thématiques. En d'autres termes, nous sommes présents sur les zones de crise où l'on pourrait être déployé ou sur des zones d'intérêt en matière de*

¹ [Audition](#) du 12 mars 2024.

² Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense.

³ [Audition](#) du 4 avril 2024.

renseignements, c'est-à-dire celles qui peuvent avoir une incidence sur les opérations menées ou qui méritent une veille particulière ».

Le travail de détection relève en revanche de la Délégation à l'information et à la communication de la Défense (Dicod) si l'offensive informationnelle vise à porter atteinte à la politique de communication des armées. Celle-ci est dotée d'un budget de 11,9 millions d'euros en loi de finances initiale pour 2024.

La Dicod s'est récemment dotée d'une capacité propre de veille sur les réseaux sociaux de campagnes de désinformation visant les armées, constituée de 6 à 7 personnes sont chargés de la veille. Lors de son audition par le rapporteur, sa directrice a également indiqué s'appuyer sur des prestataires étrangères pour cette activité de veille, par exemple pour faire remonter les contenus à partir de mots clés¹.

4. Les autres « capteurs » : services de renseignement, CIPDR...

Par nature, l'ensemble des services de renseignement concourent, chacun dans leur domaine d'expertise, à la détection d'opérations d'influences malveillantes ciblant la France :

- la DGSI s'agissant des ingérences étrangères de toutes natures sur le territoire français ;
- la DGSE, en particulier pour détecter des opérations qui viseraient des ressortissants français et les entreprises françaises qui sont exposés du fait qu'ils résident à l'étranger ;
- Tracfin, au titre du renseignement financier, qui est susceptible de détecter des canaux de financement d'opérations d'ingérences étrangères, voire des opérations de corruption ;
- la direction du renseignement et de la sécurité de la défense (DRSD) dans le domaine militaire.

Peut également être signalée la capacité de veille déployée par le secrétariat général du **comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR)**. Cette veille est réalisée par une équipe de huit agents (quatre veilleurs et quatre analystes), qui observent quotidiennement les réseaux sociaux en source ouverte, pour identifier les principaux « influenceurs » de la radicalisation islamiste en France, et peuvent donc potentiellement détecter des opérations émanant d'acteurs étrangers. Ces veilles donnent lieu à des rapports transmis aux administrations concernées et aux services de renseignement, complétant ainsi leur action.

Il convient cependant de relever que le secrétariat général du CIPDR a fait l'objet de multiples critiques, suite à des dysfonctionnements mis en

¹ *Audition du rapporteur, 25 juin 2024.*

lumière par les travaux récents de la commission des finances du Sénat¹ et de la Cour des comptes². Les décisions qui s'imposeront quant à l'avenir de cette instance devront donc également déterminer ce qu'il advient de sa capacité de veille des réseaux sociaux, en particulier au titre des influences étrangères d'inspiration islamiste.

C. UN DISPOSITIF DE COORDINATION PILOTÉ PAR LE SGDSN SELON UNE SPÉCIALISATION EN SILO DE L'ORGANISATION DE LA DÉFENSE CONTRE LES ATTAQUES HYBRIDES

C'est à titre de service du Premier ministre que le SGDSN anime et coordonne les travaux interministériels, dont les stratégies hybrides ne représentent qu'un volet parmi ses nombreuses compétences (cf. encadré).

Missions du SGDSN en application des articles R.1132-2, R.1132-3, D.1132-4 ET D.1132-7 du code de la défense

- | | |
|---|---|
| <ol style="list-style-type: none">1. Assurer le secrétariat du conseil de défense et de sécurité nationale2. Préparer la planification gouvernementale de réponses aux crises majeures3. Réagir en cas de crise4. Protéger le secret de la défense et de la sécurité nationale5. Assurer la cybersécurité et coordonner la cyberdéfense6. Assurer au Président de la République et au gouvernement les moyens de commandement et de communication électroniques nécessaires en matière de défense et de sécurité nationale et en assurer le fonctionnement7. Assurer la synthèse entre les impératifs de sécurité nationale et de protection de la vie privée8. Piloter et améliorer des dispositifs de protection | <ol style="list-style-type: none">9. Protéger le débat démocratique contre les ingérences numériques étrangères10. Piloter le contrôle des exportations de matériels de guerre11. Anticiper et suivre les évolutions internationales susceptibles d'affecter la sécurité et la défense nationale12. Participer à la préparation des décisions de haut niveau dans les domaines géopolitiques et au suivi interministériel de leur mise en œuvre13. Coordonner la lutte contre la prolifération des armes de destruction massive14. Assurer la cohérence des actions conduites en matière de sécurité économique15. Veiller à la sécurité des programmes spatiaux européens et participer à la régulation des activités spatiales |
|---|---|

Source : SGDSN

En matière de protection contre les domaines d'action hybride, les instances de coordination sont organisées selon un principe de spécialisation :

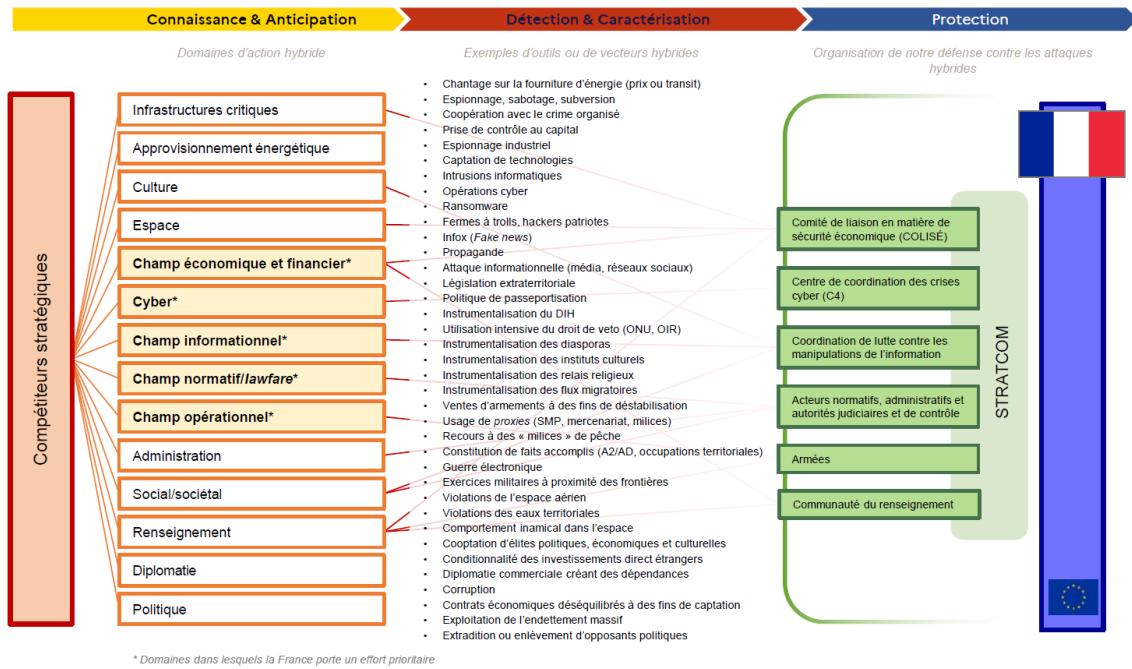
- le Comité de liaison en matière économique (Colise) ;
- le Centre de coordination des crises cyber (C4) ;
- le Colmi (comité de lutte contre les manipulations de l'information)
- les acteurs normatifs, administratifs et autorités judiciaires et de contrôle ;

¹ [Rapport d'information n° 829 \(2022-2023\)](#) fait par Jean-François Husson au nom de la mission d'information sur la création du fonds Marianne, la sélection des projets et l'attribution des subventions, le contrôle de leur exécution et les résultats obtenus au regard des objectifs du fonds, déposé le 4 juillet 2023.

² Cour des comptes, [Observations définitives sur le secrétariat général du comité interministériel de la prévention de la délinquance et de la radicalisation – Exercices 2018-2022](#), 27 novembre 2023.

- les armées ;
- la communauté du renseignement.

La coordination du SGDSN face aux menaces hybrides



Source : SGDSN

Chaque comité réunit en son sein un service chef de fil (l'Anssi pour le C4 ou Viginum pour le Colmi) et les représentants des ministères concernés : la direction générale de la sécurité intérieure (DGSI), la direction générale de la sécurité extérieure (DGSE), la direction de la communication et de la presse (DCP) du ministère de l'Europe et des affaires étrangères, le Comcyber, le pôle ASO.

A la question soulevée sur l'organisation en silo de cette coordination, le secrétaire général de la défense et de la sécurité nationale, le préfet Stéphane Bouillon a indiqué, lors de son audition par la commission d'enquête¹, que le fait qu'il présidait ces instances permettait d'en assurer également une coordination horizontale entre spécialités, mais que la déclinaison verticale des actions dépendait de chaque ministère impliqué. En tout état de cause, la réactivité et la souplesse du dispositif serait assuré par le rôle d'alerte direct du secrétaire général auprès du Premier ministre et du Président de la République, selon les matières concernées par l'urgence.

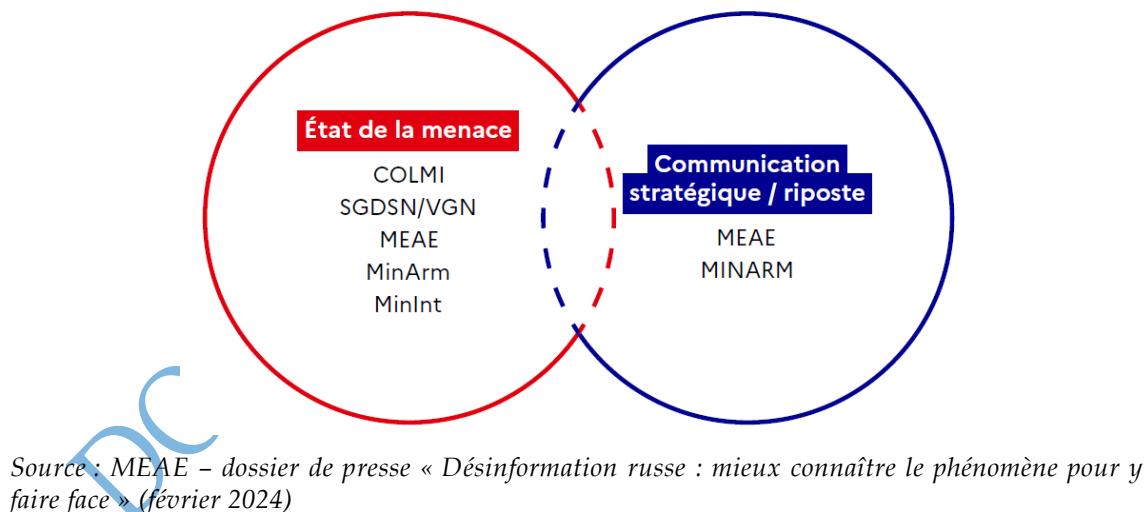
¹ [Audition](#) du 11 juin 2024.

D. UNE COORDINATION HORIZONTALE EFFICACE MAIS RESTREINTE À UN NOMBRE LIMITÉ D'ACTEURS ESSENTIELLEMENT RÉGALIENS : L'EXEMPLE DU COLMI

Dans le champ des influences malveillantes, le Colmi est donné comme un exemple de coordination étroite de la réponse française face à une ingérence numérique étrangère, en l'occurrence russes. Cette réponse implique que des acteurs étatiques examinent l'état de la menace (le SGDSN *via* Viginum et les ministères en charge des affaires étrangères, de la défense et de l'intérieur).

La communication entre ces entités en charge de la détection, de la caractérisation et, au besoin, de l'attribution (*via* des services de renseignement), avec les équipes dédiées à l'élaboration de la réponse (communication stratégique et riposte) est présenté comme un gage de réactivité et d'efficacité dans les termes suivants : « *la particularité de la France est de s'être dotée à la fois d'une agence spécialisée dans l'investigation en ligne (Viginum) et d'une équipe dédiée à la réponse en matière de crise informationnelle (Ministère de l'Europe et des affaires étrangères/État-major des armées), ce qui lui permet de couvrir un champ très large* ». *PROVISOIRE*

Schéma de coordination de la lutte contre les menaces informationnelles



La commission d'enquête a toutefois relevé une disparité de moyens entre le ministère des armées, doté d'un Comcyber intégrant l'ensemble des moyens de lutte (lutte informatique offensive [LIO], lutte informatique défensive [LID] et lutte informatique d'influence [L2I]), et le pendant civil dont ces fonctions sont réparties entre les différentes instances et ministères énumérés plus haut.

Par ailleurs, cette organisation recentrée sur les ministères régaliens ne favorise ni la sensibilisation, ni la participation d'autres ministères qui

pourraient apporter leurs contributions et leur expertise par exemple dans les domaines de la recherche et de la communication (ministères en charge de la culture et de l'enseignement supérieur).

Plus largement, le modèle français contraste avec les modèles nordiques et baltes fondés sur une approche globale de la résilience de la population et la société civile. Comment intégrer l'apport des médias et des réseaux de vérification des faits (*fact-checking*) ? Comment mutualiser la détection et partager l'information lorsque l'urgence l'exige ?

La révélation rapide au public de la manipulation de l'information autour des faux cercueils de soldats français déposés devant la Tour Eiffel (voir *Première partie, IV*) n'a été possible que grâce à la prise de conscience rapide des médias, concomitante au travail des services de l'État, quant à une possible opération d'influence étrangère. Un fonctionnement en réseau, sur le plan national mais aussi européen s'impose.

II. RÉPONSE ET RIPOSTE : OUTILS ET LIMITES DU DISPOSITIF ACTUEL

A. UNE LARGE PALETTE DE MESURES VISANT À ENTRAVER LES OPÉRATIONS D'INFLUENCE

1. De la divulgation à l'attribution : ébauche d'une communication stratégique à la française

a) La communication stratégique : transparence ou magie noire ?

Dans son ouvrage *La guerre de l'information*, David Colon définit la communication stratégique comme une « *forme de communication mise au service des objectifs stratégiques d'un État ou de son armée, en s'appuyant aussi bien sur la diplomatie publique que sur l'action psychologique pour manipuler la perception des adversaires et de leurs populations* »¹.

En matière d'influences étrangères malveillantes, la communication stratégique constitue la première mesure d'entrave. Le ministre délégué chargé de l'Europe, Jean-Noël Barrot souligne ainsi : « *Tout l'intérêt de dénoncer publiquement les opérations d'ingérence étrangère est de perturber ces opérations, sensibiliser le grand public, préparer le régime de sanctions en démontrant à nos partenaires qu'il y a lieu d'agir* ». Par nature dissimulées, les opérations de manipulation de l'information sont affaiblies par une divulgation publique qui expose leurs contenus et les force à redéployer leurs dispositifs techniques. La divulgation constitue donc le premier outil d'une palette d'instruments à la disposition des pouvoirs publics pour répondre aux influences étrangères.

¹ David Colon, *La guerre de l'information*, Tallandier Essais, 2023, p. 455.

La communication stratégique constitue historiquement une matière controversée. Dans un document transmis à la commission d'enquête, **Reporters sans frontières a souligné les limites d'un recours excessif à la notion de communication stratégique**, rappelant les échecs de sa mise en œuvre par les États-Unis lors de la seconde guerre du Golfe en 2003. Lors de son audition devant la commission, Thibaut Bruttin, adjoint au directeur général de RSF a ainsi souligné qu'« *à la magie noire de la propagande, on ne saurait cependant répondre par une autre magie noire faite de stratégies de communication* »¹.

Pour autant, la **France a engagé une mobilisation de ses différentes administrations pour répondre de manière plus offensive aux opérations d'influence malveillantes** et en particulier aux manipulations de l'information. Chronologiquement, cette mobilisation a été amorcée dans le champ des armées du fait, comme expliqué *supra*, de la multiplication des attaques informationnelles visant les opérations extérieures. **Le domaine militaire s'est donc trouvé dans une position plus exposée que le domaine civil des affaires étrangères**².

Depuis plusieurs mois, le **ministère de l'Europe et des affaires étrangères (MEAE)** s'est cependant **vu doté de davantage de moyens de riposte informationnelle et d'un mandat politique clair** pour contrer les opérations d'influence malveillantes. Dans son discours prononcé à l'occasion de la conférence des ambassadrices et des ambassadeurs, le 1^{er} septembre 2022, le président de la République a engagé la diplomatie française à s'engager pleinement dans la réponse aux attaques informationnelles : « *je compte vraiment sur vous toutes et tous et sur le réseau pour vous mobiliser dans cette stratégie d'influence, et, vous le voyez bien aussi, de contre-influencer pour combattre les narratifs mensongers, les informations fausses et défendre la réalité de notre action* »³. Toutefois, au regard des objectifs affichés, la commission estime que les moyens du ministère sont encore insuffisants pour assurer une veille et une riposte efficace.

b) La communication stratégique du ministère de l'Europe et des affaires étrangères

La riposte du ministère de l'Europe et des affaires étrangères aux opérations de manipulation de l'information **se trouve facilitée lorsque la désinformation est assumée et portée directement par un État étranger**.

Depuis février 2022, la communication publique agressive engagée par la diplomatie russe fait l'objet de **réponses plus fréquentes de la part des diplomates français**. En juin 2024, l'ambassade de Russie en Afrique du Sud

¹ [Audition du 13 juin 2024](#).

² Nicolas Barotte, « [Dans la guerre d'influence, les militaires attendent l'appui du Quai d'Orsay](#) », Le Figaro, 1^{er} septembre 2022, en ligne, consulté le 5 juillet 2024.

³ [Discours du président de la République Emmanuel Macron à l'occasion de la conférence des ambassadrices et des ambassadeurs](#), 1^{er} septembre 2022.

a ainsi relayé une vidéo présentée comme la capture par l'armée russe d'un mercenaire français en Ukraine. Les images montrent un homme en uniforme laissant apparaître clairement un drapeau français se rendre à des soldats russes en criant, avec un fort accent « *Ne tirez pas !* ». En réponse, l'ambassade de France en Afrique du Sud a répliqué à son homologue russe sur le même réseau social : « *Chers collègues, vous diffusez depuis un certain temps de fausses nouvelles et nous sommes désormais habitués à cette pratique peu diplomatique. Cependant, celle-ci est particulièrement ridicule. Nous proposons à vos comédiens de travailler leur accent avec quelques cours de français à l'Alliance française* ».

De manière plus large, au-delà d'opérations de manipulation de l'information ponctuelles, qu'elles soient dissimulées ou ouvertement portées par un État étranger, la diplomatie française tente de renforcer sa présence communicationnelle pour contrer le « *bruit de fond* » de la désinformation.

Le renforcement de la communication stratégique du ministère s'est notamment traduit par la nomination en août 2022, d'une Ambassadrice pour la diplomatie publique en Afrique, en la personne de Mme Anne-Sophie Avé. La création d'une nouvelle ambassade thématique poursuivait un double objectif, précisé par sa lettre de mission :

- d'une part, valoriser les actions de la France en rendant « *davantage visibles et audibles* » les efforts de la France pour renouveler son partenariat avec l'Afrique. Cette mission correspond à un renforcement des actions de communication stratégique au sein des ambassades, d'élaboration d'un narratif de référence et de recours renforcé à des relais locaux ;

- d'autre part, riposter aux attaques informationnelles visant la France en Afrique par une structuration des dispositifs de veille et d'alerte et la coordination des stratégies de riposte. En ce sens, l'ambassadrice se voyait charger de préparer les orientations des argumentaires de riposte et d'évaluer les dispositifs existants.

La mise en œuvre de cette double mission par l'ambassadrice pour la diplomatie publique en Afrique a conduit à harmoniser les éléments de réponse aux attaques informationnelles. Plusieurs fiches repères de réponse aux principaux axes de dénigrement de la France en Afrique, comme le Franc CFA, l'industrialisation du continent, le panafricanisme et la délivrance des visas ont été produites et diffusées au sein du réseau diplomatique. De plus, des éléments de formation aux médias et à la communication ont également été fournis.

Si la nomination d'une ambassadrice thématique a permis de mieux identifier le déficit de moyens du MEAE pour riposte aux attaques d'influence et de coordonner des éléments de riposte, il apparaît néanmoins que cette réponse n'était qu'embryonnaire par rapport au volume de la menace. En particulier, les moyens de production de contenu informationnel, que la commission d'enquête a pu consulter, s'avéraient nettement insuffisants. Les

effectifs limités, de l'ordre de trois équivalents temps plein (ETP)¹, ne permettaient un soutien effectif aux postes. **Les productions de ses équipes ont donc été limitées.**

Les missions de l'ambassadrice pour la diplomatie publique en Afrique ont vocation, selon l'ambassadrice elle-même, d'être reprises par la direction de la communication du ministère de l'Europe et des affaires étrangères. La logique du travail de cette ambassade thématique **s'inscrivait dans le cadre d'une administration de mission** : « *Si le président de la République m'a nommée à ce poste, c'est sans doute pour insister sur cette difficulté et souligner le travail de coordination qu'il convenait de mener ; mais, à terme, chacun, dans son domaine, doit reprendre l'ensemble de ses missions, dans le cadre, bien sûr, d'une action coordonnée* »².

En effet, la structuration progressive de la sous-direction veille et stratégie (VS), placée au sein de la direction de la communication et de la presse (DCP) du ministère de l'Europe et des affaires étrangères, à partir d'août 2022 a permis de renforcer les capacités de riposte du Quai d'Orsay. **Il convenait en effet de créer, au sein du ministère, un service chef de file sur la veille et la riposte aux offensives informationnelles.** Outre un pôle chargé de la veille des médias et un pôle chargé de la veille des réseaux sociaux, qui interviennent en complément de l'action de Viginum, **cette sous-direction comprend également un pôle en charge de la communication stratégique.**

La mission de la sous-direction VS vise à protéger le réseau diplomatique français et à **mener des actions contre les atteintes réputationnelles à l'encontre de la France à l'étranger**. Dans le prolongement de ses activités de veille, le service analyse les éléments constitutifs de la manœuvre informationnelle pour élaborer des éléments de réponse, en coordination avec les représentations diplomatiques françaises concernées. Selon le ministre de l'Europe et des affaires étrangères, Stéphane Séjourné « *En dix-huit mois, nous avons instauré à Paris et dans les ambassades une logique de riposte, pour rétablir les faits de manière rapide et agile par tous les moyens. Il s'agit aussi de lutter contre la dénonciation publique en recourant à cette même méthode* »³.

Lors de la crise survenue au Niger en juillet 2023, la suite d'un coup d'État contre le président Mohamed Bazoum, **l'action combinée de la sous-direction aurait permis de désamorcer une quarantaine de campagnes de désinformation visant les intérêts français dans le pays.** Cette action s'est traduite par la publication de contenus sur les réseaux sociaux visant à rétablir les faits auprès d'une série d'acteurs.

¹ Un agent du ministère des armées, un contractuel et un stagiaire du ministère de l'Euro, non renouvelés.

² [Audition](#) du 30 avril 2024.

³ [Audition](#) du 18 juin 2024.

Dans une logique plus préventive et, en cohérence avec les missions qui étaient assurées par l'ambassadrice pour la diplomatie publique en Afrique, la sous-direction veille et stratégie dispose également d'une compétence de formation des ambassades aux enjeux de la désinformation. Ces mesures de formation s'accompagnent d'un renforcement des capacités de veille et de riposte dans les postes diplomatiques. La création de 123 nouveaux ETP a permis de doter l'ensemble des ambassades d'un service de presse.

2. Les mesures d'entrave dans le champ des armées

a) La réponse aux opérations informationnelles visant les forces françaises déployées sur un théâtre extérieur

En parallèle de la communication stratégique du MEAE, le ministère des armées a également structuré et renforcé ses capacités de riposte communicationnelle. Les actions de riposte des armées s'inscrivent dans le cadre de la lutte informatique informationnelle (L2I). Ces opérations militaires visent à contrer les attaques susceptibles de nuire aux forces françaises et à promouvoir l'action de ces dernières.

Ces actions peuvent promouvoir la communication stratégique des armées française définie par la doctrine interarmées du 23 juin 2014, révisée en 2018, comme le « *processus qui permet de cadrer la conception et la conduite de toute activité militaire des armées françaises comme un message cohérent, crédible et efficace auprès des principaux acteurs qui en ont connaissance, qu'il s'agisse d'une action physique ou d'une prise de parole sous toutes ses formes* ».

La mission de lutte informationnelle, menée par le commandement de la cyberdéfense (Comcyber) sous l'égide de la cellule « *anticipation stratégique et orientation* » (ASO) de l'état-major des armées, s'opère en parallèle mais distinctement des fonctions de riposte informationnelle du MEAE. Le Comcyber n'intervient en effet que dans le champ militaire et hors du territoire national. Seul Viginum est compétent pour la protection du débat public numérique français. La stricte prohibition faite aux armées d'intervenir sur le territoire national en matière informationnelle paraît nécessaire à la commission d'enquête. Comme l'a souligné le ministre des armées Sébastien Lecornu lors de son audition : « *Rappelez-vous l'armée française qui, pendant la guerre d'Algérie, distribuait des tracts pour expliquer à quel point c'était bien que l'Algérie soit un département français. Avec le recul, peut-on dire que c'était la mission de l'armée française que de mener ce combat de conviction ? Non, à la rigueur, c'était un combat politique* »¹. Pendant la guerre d'Algérie, un service spécialisé dans la guerre psychologique, le 5^{ème} bureau de l'état-major, avait en effet été créé en 1957 pour mener des

¹ [Audition](#) du 25 juin 2024.

actions de propagande et de contrôle des populations. Compte tenu des dérives observées, ce service est dissous en 1960.

En outre, le champ d'intervention matériel du Comcyber est plus étendu que la mission de communication stratégique confiée à la direction de la communication et de la presse. Il comprend une dimension additionnelle qui permet à nos forces armées de mener des actions de déception de l'adversaire.

Toutefois, en présence d'une crise informationnelle grave, les moyens du MEAE et de la cellule ASO peuvent être mis en commun au sein de la task force interministérielle informationnelle (TF2I). Au-delà du rétablissement rapide des faits face à une intox, la task force coordonne des campagnes de communication stratégique plus structurées à l'international. Sur les questions de lutte contre les manipulations de l'information, son intervention s'articule avec l'action du comité interministériel de lutte contre les manipulations de l'information (Colmi). Pour ce faire, Viginum peut assister en tant qu'observateur à la TF2I.

Les moyens d'intervention des armées relèvent ainsi de trois ordres.

En premier lieu, les forces françaises peuvent recourir aux leviers de la communication stratégique pour contrer une attaque informationnelle. Il s'agit de dénoncer l'opération en cours auprès d'auditoires d'intérêt et de rétablir la vérité pour éviter une propagation de la désinformation. En ce sens des actions de démythification (« *debunking* ») et de vérification de l'information sont menées, le plus rapidement possible. Selon le général Bonnemaison, commandant de la cyberdéfense de l'état-major des armées, « *l'enjeu étant de le faire dans des délais suffisamment restreints pour qu'elle ne puisse pas porter ses fruits* »¹. Ce mode d'action présente toutefois des limites, propres à toute dénonciation d'une fausse information, en ce que le narratif peut demeurer disponible avec une propagation résiduelle.

Ce rôle de communication stratégique accompagne les armées à chaque instant. Comme le précise en effet le général Bonnemaison : « *dès que l'on part en opération – par exemple, le déploiement d'une force navale –, nous accompagnons ce déplacement d'un narratif valorisant l'action et la présence des forces françaises et nous veillons aussi aux effets négatifs* ».

En deuxième lieu, il est possible de recourir à des leviers situés hors du ministère des armées pour faire cesser une campagne de désinformation sur les plateformes, notamment en activant la voie diplomatique ou en saisissant la plateforme Pharos. Ces mécanismes sont décrits *infra*.

En troisième lieu, les armées peuvent recourir à des actions de déception sur lesquelles la commission d'enquête, tenue par le secret de la défense nationale, s'en tient à la discréetion.

¹ [Audition](#) du 4 avril 2024.

Il importe néanmoins de préciser sur ce point que **les interventions de la France se font dans un cadre juridique strict**. Les actions militaires dans la sphère informationnelle se font dans le respect du droit interne et du droit international, comme le rappelle la doctrine de lutte informatique d'influence de 2021 :

- en temps de paix, **les opérations respectent le droit international et les principes de la Charte des Nations unies** et en particulier le principe de non-ingérence ;
- dans un conflit armé, **ces actions respectent le droit international humanitaire** et notamment les principes de distinction, de nécessité militaire et de proportionnalité.

Chaque opération du Comcyber est encadrée par des règles opérationnelles d'engagement (ROE), validées le chef d'état-major des armées. Deux conseillers juridiques (« *legads* »), un opératif et un auprès du chef de corps, interviennent sur chaque opération.

La France se distingue par des **principes détaillés d'encadrement de ses engagements en matière informationnelle par sa doctrine de L2I**, d'une part, et en s'appuyant sur un manuel de droit international appliqué aux opérations dans le cyberspace. Ces documents, sans préciser l'ensemble des actions de la France, indique celles dont elle s'interdit l'usage, comme les manipulations de l'information.

Pour mener des opérations de déception, le Comcyber **s'appuie essentiellement sur la distinction opérée par le droit international entre la ruse, autorisée, et la perfidie, prohibée**. Cette distinction est établie par l'article 37 du protocole additionnel aux conventions de Genève.

D'une part, **l'interdiction de la perfidie constitue une règle fondamentale de la conduite du combat**¹. L'article 37 du protocole additionnel aux conventions de Genève stipule que « *constituent une perfidie les actes faisant appel, avec l'intention de la tromper, à la bonne foi d'un adversaire pour lui faire croire qu'il a le droit de recevoir ou l'obligation d'accorder la protection prévue par les règles du droit international applicable dans les conflits armés* ». Il est par exemple **interdit de feindre un statut protégé**, en usant du signe de la croix rouge par exemple. Dans le contexte de la lutte informatique informationnelle, la perfidie correspondrait au fait de se faire en ligne pour une ONG ou un mineur.

D'autre part, **le recours à la ruse est autorisé par le droit international humanitaire**. Pour le protocole additionnel aux conventions de Genève, « *constituent des ruses de guerre les actions qui ont pour but d'induire un adversaire en erreur ou de lui faire commettre des imprudences, mais qui*

¹ Comité international de la Croix-Rouge, *Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I)*, 8 juin 1977. *Commentaire de 1987, Bases de données de droit international humanitaire*.

n'enfreignent aucune règle du droit international applicable dans les conflits armés, et qui ne faisant pas appel à la bonne foi de l'adversaire en ce qui concerne la protection prévue par ce droit, ne sont pas perfides ». Se faire passer pour un adversaire pour l'induire en erreur, diffuser un faux itinéraire de convoi logistique ou une fausse position d'aéronef est par conséquent possible.

L'affaire dite du « *charnier de Gossi* » **constitue un exemple d'opération de déception menée par les armées dans le champ informationnel**. Dans le contexte du départ des forces françaises du Mali, décidé en février 2022, la base militaire de Gossi est restituée le 19 avril 2022 aux forces armées malientes. Anticipant une manœuvre informationnelle des forces malientes et du groupe Wagner, **l'armée française a décidé de faire survoler la base par un drone de surveillance**. Ce dernier détecte et filme durant une journée les hommes de Wagner en train de constituer un faux charnier sur le terrain de la base, dans le but d'accuser la France de crimes de guerre. La France a toutefois attendu le déclenchement d'une campagne de désinformation en ligne, au travers d'un compte Twitter « *Dia Diarra* » présentant les premières images du charnier, **pour fournir à la presse les informations dont elle disposait**. Immédiatement démentie, cette opération d'influence malveillante a pu être stoppée. **En attendant le dernier moment pour divulguer et attribuer cette manœuvre a fait usage de ruse pour induire en erreur l'adversaire**.

Constitution du faux charnier de Gossi par le groupe Wagner filmé par un drone français



Source : ministère des armées

Par ailleurs, il importe de souligner que les actions de lutte informationnelles des armées peuvent se combiner avec des actions de lutte informatique défensive et de lutte information offensive. Cette combinaison découle de la nature même des attaques visant nos forces. Une opération de piratage et de divulgation nécessitera une réponse sur le plan cyber et une réponse sur le champ informationnel. Ceci justifie le regroupement des actions cyber et informationnelle dans une même unité, s'agissant des armées.

b) La réponse aux opérations informationnelles visant les armées françaises et la politique de défense française

En sus des opérations informationnelles visant les forces françaises déployées sur un théâtre extérieur, qui relèvent du Comcyber, certaines opérations ciblent plus largement les armées françaises en tant qu'institution et la politique de défense française de manière générale. En ce qu'elles portent atteinte à la communication des armées, la réponse à ces attaques relèvent de la délégation à l'information et à la communication de la Défense (Dicod), dont la directrice Olivia Pénichou a été auditionnée par le rapporteur¹.

Comme indiqué *supra*, la Dicod s'est dotée d'un dispositif de veille et d'alerte propre, qui lui permet d'être en mesure de proposer rapidement au ministre des armées de répondre publiquement aux attaques.

Le ministre des armées Sébastien Lecornu a donné lors de son audition par la commission d'enquête² deux exemples récents d'opérations ayant fait l'objet d'une dénonciation publique de sa part :

- le 15 mars dernier, des acteurs pro-russes ont usurpé un nom de domaine officiel de recrutement de l'armée française pour créer le site *sengager-ukraine.fr*, afin de faire croire que la France allait déployer des troupes en Ukraine. Selon le ministre, l'opération visait ainsi à donner « une forme de crédit à une fausse information et détournant la parole du président de la République, qui, au moyen d'un verbatim précis, a voulu créer ce qu'on appelle une ambiguïté stratégique. Évidemment, les Russes en ont profité pour faire pencher l'ambiguïté du côté qui les intéressait, en suscitant un débat en politique intérieure française » ;

- l'annonce de Russie selon laquelle des militaires français auraient trouvé la mort dans une frappe en Ukraine publiant sur les réseaux sociaux la liste de ces militaires. Or, comme l'a précisé le ministre : « il se trouve que les militaires dont les noms apparaissaient sur cette liste avaient bien mis les pieds en Ukraine, au cours non pas des deux dernières années, mais des dix dernières années ! C'étaient également des techniciens informatiques qui étaient venus réparer les ordinateurs de la mission de défense de notre ambassade de Kiev, des militaires ayant accompagné telle ou telle mission parlementaire, etc. Certains d'entre eux sont même actuellement à la retraite ! En quatre ou cinq jours, nous avons pu indiquer à quand remontait, pour chacune des personnes présentes sur cette liste, son dernier séjour en

¹ *Audition du rapporteur, 25 juin 2024.*

² *Audition* du 25 juin 2024.

Ukraine ». Le ministère a donc publié un communiqué dénonçant une « *manœuvre coordonnée de la Russie* »¹.

Par ailleurs, la Dicod anime une communauté des communicants de la défense, et s'efforce de structurer les relations qu'elle entretient avec la presse, pour faire état des campagnes de désinformation ciblant les armées qu'elle détecte, par l'organisation de rencontres régulières.

La Dicod publie désormais à leur intention une « *Newsletter de la désinformation* », et a publié récemment un *Guide contre de la désinformation*².

3. Les actions des services de renseignement

S'agissant des actions mises en œuvre par les services de renseignement pour entraver des actions d'influence malveillantes, les détails et statistiques des opérations sont couverts par le secret de la défense nationale. La commission d'enquête renvoie par conséquent aux rapports publics relatifs à l'activité de la délégation parlementaire au renseignement publiées par cette dernière.

4. Les actions diplomatiques de nature à faire cesser une opération d'influence

a) Auprès des États

Des mesures diplomatiques peuvent contribuer à mettre fin à une opération d'influence malveillante.

D'une part, l'**ambassadeur du pays à l'initiative de cette opération peut faire l'objet d'une convocation par le ministre de l'Europe et des affaires étrangères pour explication**. En mars et en avril 2022, le ministre de l'Europe et des affaires étrangères Jean-Yves Le Drian a ainsi convoqué à deux reprises l'Ambassadeur de Russie en France pour protester contre la communication de l'ambassade sur le conflit en Ukraine. Le 25 mars 2022, l'Ambassadeur avait dû s'expliquer sur une caricature dénigrant l'Union européenne relayée par le compte Twitter de l'ambassade. De même, le 7 avril 2022, la **convocation visait à condamner une publication par le compte Twitter de l'ambassade qui présentait la découverte du massacre de Boutcha en Ukraine comme une mise en scène**. À ces deux occasions, l'ambassade a procédé au retrait de ces publications. La convocation d'un ambassadeur peut ne pas être rendue publique.

D'autre part, **des diplomates étrangers peuvent faire l'objet d'une procédure d'expulsion et être déclarés *persona non grata***. À cet égard, la

¹ Ministère des armées, [Communiqué de presse – Manœuvre de désinformation russe](#), 26 janvier 2024.

² Ministère des armées, [Guide contre la désinformation](#).

convention de Vienne sur les relations diplomatiques stipule que « *L'État accréditaire peut, à tout moment et sans avoir à motiver sa décision, informer l'État accréditant que le chef ou tout autre membre du personnel diplomatique de la mission est persona non grata ou que tout autre membre du personnel de la mission n'est pas acceptable* »¹. En avril 2022, la France a opéré l'expulsion de 41 diplomates russes, présentés par le Quai d'Orsay comme des « *agents russes agissant sur notre territoire sous un statut diplomatique et œuvrant contre nos intérêts de sécurité* ».

b) Auprès des plateformes

Le ministère de l'Europe et des affaires étrangères peut engager un dialogue avec les plateformes numériques pour demander le retrait de contenus qui sembleraient relever d'une opération de manipulation de l'information visant la France.

À ce titre, **l'Ambassadeur pour le numérique assure une fonction de dialogue stratégique avec les grandes plateformes**. Ces échanges visent en premier lieu à défendre, auprès de ces entreprises, les positions de la France sur les grands enjeux du numérique. Cependant, comme l'expose l'Ambassadeur Henri Verdier, il peut également solliciter les solliciter pour demander la suppression de certains contenus : « *Nous dialoguons, à la fois, sur des principes ou des controverses, comme la définition d'un comportement inauthentique ou la promotion des meilleures pratiques, et, de manière semi-opérationnelle, lorsque des acteurs comme le ministère des armées, le service de vigilance et protection contre les ingérences numériques étrangères (Viginum) ou la DCP me demandent de signaler ou d'insister sur l'importance de certaines désinformations, surtout en période de crise* »².

Cette sollicitation diplomatique **intervient donc dans l'hypothèse où les plateformes ne supprimerait pas d'elles-mêmes les contenus révélés par Viginum ou un autre service**. Les rapports techniques publiés par Viginum constituent à cet égard un levier conséquent pour inciter les plateformes à endiguer la diffusion des contenus concernés. Ces documents, qui s'appuient sur une méthodologie solide et transparente, **présentent clairement les éléments permettant de caractériser une ingérence numérique étrangère**. Il s'agit pour la diplomatie française avant tout de demander aux plateformes d'appliquer leurs conditions d'utilisation.

Les leviers juridiques dont disposent la diplomatie française sont néanmoins limités. En dépit de signalements fréquents réalisés par le MEAE pour alerter sur des contenus de désinformation ou pouvant porter atteinte à des questions de sécurité des emprises ou des agents diplomatiques, **il est fréquent que les grands groupes du numérique oppose à la France une fin de non-recevoir**. Ainsi, on peut signaler :

¹ Article 9 de la convention sur les relations diplomatiques du 18 avril 1961, confirmé par l'article 23 de la convention du 24 avril 1963 sur les relations consulaires et les accords de siège.

² [Audition](#) du 28 mars 2024.

- le **refus de Twitter/X de supprimer des comptes ayant participé à de nombreuses manœuvres de désinformation** et de *doxxing*¹, notamment concernant la présence militaire française et son prétendu rôle dans la formation des djihadistes au Sahel ;

- le **refus de Twitter/X de supprimer plusieurs contenus** signalés qui relaient un faux audio attribué au président de la République en août 2023 affirmant que le Gabon serait dirigé par un imposteur ;

- le **refus de Meta de supprimer plusieurs publications signalées en août 2023** qui partagent un faux document présenté comme un OPO (ordre militaire) visant à une invasion du Niger par la France et ses alliés. Le document comprend des erreurs de forme évidentes et mentionne des unités qui n'existent pas ;

- le **refus de Twitter/X de supprimer des contenus** qui lui ont été signalés en décembre 2023 affirmant à tort que des militaires français seraient présents aux côtés de l'armée israélienne dans la bande de Gaza ;

- le **refus de Twitter/X de supprimer des relais francophones d'un article de Sputnik** de janvier 2024 alléguant sans aucun élément de preuve que des mercenaires français auraient été tués dans une frappe russe près de Kharkiv.

Les différentes auditions menées par la commission d'enquête ont souligné **le refus de la plupart des grandes plateformes numériques de coopérer avec les pouvoirs publics s'agissant de la désinformation en ligne**. Le ministre de l'intérieur et des Outre-mer, Gérald Darmanin, a ainsi indiqué à la commission que « *La coopération avec les plateformes est difficile et inégale. Je veux saluer notre travail avec Meta, qui montre un certain entrain, depuis plusieurs mois désormais, à répondre à la loi française. Nous rencontrons plus de difficultés avec d'autres plateformes, notamment TikTok et X* »².

À ce sujet, lors de son audition, la directrice des affaires publiques de X France a indiqué à la commission d'enquête être, avec le directeur de X France, les deux seuls « *point de contact* » pour les autorités françaises. Si la directrice a pu contester les propos du Ministre, en déclarant qu'elle « *était en contact avec les forces de l'ordre et Pharos, dont certains membres ont mon numéro de téléphone personnel* » et qu'ils « *s'efforçaient de [se] rendre disponibles, dans la mesure de [leurs] moyens, vis-à-vis du ministère de l'intérieur* », elle a également reconnu que les équipes des directions des affaires publiques étaient souvent limitées. En réponse au président de la commission d'enquête, qui a tenu cette déclaration pour « *un aveu que X ne se donne pas les moyens de ses ambitions en matière de conformité et de collaboration avec les autorités en charge de la*

¹ Méthode de divulgation de données personnelles.

² [Audition](#) du 28 mai 2024.

régulation », la directrice a expliqué que le défaut de recrutements était lié à la situation financière de l'entreprise, qui n'a jamais été rentable¹.

5. La saisine de la plateforme Pharos

Au-delà d'une demande diplomatique, le recours à la plateforme de signalement Pharos, créée par un arrêté du 16 juin 2009 et gérée par l'Office anti-cybercriminalité (Ofac), peut permettre de solliciter auprès des plateformes le retrait de contenus s'apparentant à des opérations d'influence malveillantes. Cette plateforme centralise les signalements des particuliers et des associations, qui ont valeur de renseignement et qui peuvent justifier l'ouverture d'une enquête. En application de l'article 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, Pharos peut notamment demander à l'hébergeur le retrait de contenus contrevanant aux articles 421-2-5 et 227-23 du code pénal² et aux moteurs de recherche le déréférencement d'adresses électroniques présentant de tels contenus.

Pharos dispose à cet effet d'un portail en ligne ouvert aux particuliers. Elle échange, en outre, avec d'autres services de l'État dont les services de veille, autorités administratives indépendantes ou services de renseignement sur les contenus illicites hébergés en ligne. À ce titre, Pharos a signé le 7 décembre 2023 une convention de partenariat avec le service Viginum, faisant de ce dernier un partenaire référencé.

Toutefois, le champ d'intervention de Pharos est limité à un domaine précis. Il s'agit des cas d'appels à la violence, appel à la haine, terrorisme, trafic illicite, incitation à commettre des infractions, escroquerie, injure ou diffamation. Le contenu des opérations de désinformation, notamment celles conduites par la Russie à l'encontre de la France, veille à rester sous le seuil de l'incitation à la haine.

Les ingérences numériques étrangères (INE) définies par le décret n° 2021-922 du 13 juillet 2021 portant création de Viginum ne relèvent ainsi pas du domaine de Pharos, qui n'assure par conséquent aucune quantification de ce phénomène. De même, la plateforme n'est pas compétente *stricto sensu* pour traiter des fausses informations, qui ne sont pas illicites, à moins qu'elles ne s'inscrivent dans un cadre électoral.

Cela étant, un certain nombre de signalements transmis à la plateforme Pharos peuvent se rattacher à la thématique des influences étrangères malveillantes. À titre d'exemple, en 2023 et en 2024, la plateforme a reçu des signalements en lien avec des opérations de désinformation sur la présence militaire française en Afrique. Ces actions reposaient sur la diffusion de faux documents officiels français prévoyant des remises d'armes

¹ [Audition](#) du 30 mai 2024.

² Soit la provocation à des actes de terrorisme et la pédocriminalité.

à des terroristes. De même, en mars 2024, Pharos a été saisie de l'affaire du faux site du ministère des armées « sengager-ukraine.fr ».

6. L'opportunité de la riposte aux attaques informationnelles d'influence

Pour autant, **la décision de divulguer et d'attribuer une opération d'influence étrangère n'est systématique**. Pour le ministre délégué chargé de l'Europe, Jean-Noël Barrot, « *La décision de dénoncer publiquement sera mesurée à l'aune de toutes les dimensions diplomatiques. En d'autres termes, la dénonciation publique ne sera pas automatique* »¹. Selon les circonstances et la nature de l'opération, il peut être préférable de recourir à d'autres mesures d'entraves.

En tout état de cause, **compte tenu de l'implication d'un acteur étranger, des travaux de coordination en interministériel sont indispensables à la formulation d'une riposte**. Cette coordination est assurée par le comité interministériel de lutte contre les manipulations de l'information (Colmi). Cette instance, placée sous la conduite du secrétariat général de la défense et de la sécurité nationale (SGDSN), a succédé au comité interministériel ad hoc qui se réunissait deux fois par ans entre 2018 et 2021. Par rapport au précédent format, **le Colmi comporte une dimension opérationnelle plus poussée, sur le modèle du Centre de coordination des crises cyber (C4)**, en ce qu'il formule les options de réponse aux opérations de manipulation de l'information.

Le Colmi regroupe, sous l'égide du SGDSN, le ministère des armées, le ministère de l'intérieur et des Outre-mer et le ministère de l'Europe et des affaires étrangères. **Au niveau du Colmi-tech**, il s'agit :

- du Comcyber et de la direction générale de la sécurité extérieure (DGSE) pour le ministère des armées ;
- de la direction générale de la sécurité intérieur (DGSI) pour le ministère de l'intérieur et des Outre-mer ;
- de la sous-direction « veille et stratégie » de la direction de la communication et de la presse pour le ministère de l'Europe et des affaires étrangères ;
- de Viginum, pour le SGDSN, qui en assure l'animation.

Il se réunit **une fois par semaine sous le format Colmi-tech** pour examiner la liste des opérations signalées par Viginum. **Une fois par mois, un Colmi plus complet se réunit sous la présidence du SGDSN**. À l'issue de ces réunions, un document est adressé aux cabinets des ministres concernés qui propose aux ministres concernés l'imputation ou l'attribution des dossiers détectées et précise le calendrier des opérations.

¹ [Audition](#) du 29 mai 2024.

L'arbitrage entre les différentes options proposées par le Colmi se fait au niveau politique le plus élevé. Selon le secrétaire général de la défense et de la sécurité nationale, Stéphane Bouillon, cette décision remonte jusqu'au Président de la République¹. Si la décision de riposter ou non à une opération d'influence, compte tenu de ses enjeux diplomatiques, nécessite un arbitrage politique au plus haut niveau, **la commission d'enquête s'étonne de la mise à l'écart du Premier ministre, pourtant « responsable de la défense nationale »** et chargé de la direction de l'action du Gouvernement, en application de l'article 21 de la Constitution. Certes, le secrétaire général de la défense et de la sécurité nationale a indiqué à la commission d'enquête que cette décision était prise « *en lien avec Matignon* », pour autant le portage politique au niveau interministériel paraît très insuffisant.

De plus, il apparaît qu'il n'existe, à ce stade, aucune doctrine de réponse face aux attaques informationnelle d'influence. Si les auditions menées par la commission d'enquête ont permis de déceler quelques éléments d'orientation tirés de l'expérience des participants au comité interministériel, aucune ligne de conduite n'est formellement déterminée. **Il s'agit avant tout d'une approche empirique.**

La décision de révéler et d'attribuer à un État une opération d'influence n'est ainsi pas automatique. La campagne azerbaïdjanaise *Olympiya*, par exemple, n'a fait l'objet d'aucune communication officielle de la part du Gouvernement. Son existence et ses liens avec le régime illibéral de Bakou ont été rendus publics par la presse qui a pu avoir accès aux éléments techniques produits par Viginum de manière officieuse. **Pour différentes raisons, en particulier diplomatiques, il peut être préférable pour la France de ne pas communiquer sur une opération, tout en prenant des mesures plus discrètes** pour y mettre un terme. Comme l'indique l'Ambassadeur pour le numérique Henri Verdier, « *en plus des attributions publiques, les attributions privées sont possibles. Il m'est arrivé de tenter de construire un dialogue stratégique en Russie ou en Chine, au travers duquel beaucoup de choses se disent, mais dans des enceintes privées* »².

La principale raison motivant le silence gardé sur la détection d'une opération d'influence est de ne pas accroître sa visibilité. Il s'agit d'**éviter l'« effet Streisand » en attirant l'attention sur une opération de manipulation** de l'information dont l'audience ne serait pas forcément aussi étendue que l'on croit. Dès lors que l'on n'est pas en mesure d'évaluer précisément l'audience et l'impact d'une opération d'influence, **braquer l'attention du public et des médias son existence soulève un risque de retour de bâton.** Cette amplification involontaire d'une action de désinformation peut servir l'adversaire qui donne alors l'illusion d'une force de frappe plus importante qu'elle ne l'est réellement. Comme souligné lors de l'introduction, **l'un des**

¹ [Audition](#) du 10 juin 2024.

² [Audition](#) du 28 mars 2024.

objectifs des stratégies d'influence agressives de nos compétiteurs est de faire douter nos concitoyens de la solidité de nos démocraties.

De plus, la révélation des opérations d'influence **ne met pas forcément un terme à leur déroulement**. S'agissant de l'opération *Portal Kombat*, dénoncée par la France en février 2024, des comptes liés à cette campagne sont toujours activité et Viginum continue de cartographier l'étendue du réseau de cette manœuvre informationnelle. **Dans la majorité des cas, toutefois, la dénonciation semble constituer le moyen le plus efficace pour y mettre un terme, à condition d'agir rapidement**. En tout état de cause, la dénonciation permet d'imposer des coûts d'adaptation à l'attaquant :

- d'une part, **en le forçant à adapter son dispositif**, voire une évolution de sa manœuvre, par exemple en investissant dans de nouveaux noms de domaines ;
- d'autre part, plus indirectement, une fois l'opération caractérisée, **la dénonciation publique peut donner lieu à des sanctions**, notamment au niveau de l'Union européenne, comme cela sera exposé *infra*.

Par ailleurs, outre ces effets opérationnels, la divulgation **contribue à l'information du public et à sa prise de conscience de la menace liée aux opérations d'influence**. Ces dernières deviennent plus tangibles pour les citoyens et les encouragent dans une approche de résilience à faire preuve d'esprit critique.

Lorsque la décision est prise de dénoncer une opération d'influence, le ministère de l'Europe et des affaires étrangères, chef de file sur la fonction d'influence à l'extérieur, est chargé d'assurer la communication. Dans le cas d'une campagne informationnelle d'ampleur, **la task force interministérielle informationnelle est mobilisée pour préparer et coordonner la réponse de l'État en termes de communication stratégique**.

Toutefois et l'absence de doctrine de réponse consolidée, lorsque l'opération concerne plus spécifiquement le champ d'un autre ministère, ce dernier peut assurer la dénonciation publique de l'attaque. En ce sens, l'Ambassadeur Henri Verdier a précisé à la commission d'enquête que « *La réponse dépendant du sujet, notre doctrine tend effectivement à la confier au ministère compétent, à celui qui est le plus attaqué – le ministère de l'Europe et des affaires étrangères va intervenir sur les affaires internationales ou celles qui concernent nos armées sur un théâtre d'opérations extérieures, pas sur une rumeur concernant le monde agricole* »¹.

Les opérations d'influence font donc l'objet **d'une dénonciation et d'une attribution par le ministre compétent « au fond » de la politique publique visée**. Trois exemples récents peuvent être cités :

¹ [Audition](#) du 28 mars 2024.

- la mise à jour du réseau d'influence *Portal Kombat*, principalement destiné à soutenir l'« opération militaire spéciale » russe en Ukraine, a été annoncée le 12 février 2024 par le ministre de l'Europe et des affaires étrangères Stéphane Séjourné. Dans le prolongement de cette annonce, le SGDSN rendait public un rapport technique consacré à cette opération et étayant l'attribution de sa conduite à la Russie¹ ;

- les manœuvres d'influence de l'Azerbaïdjan en Nouvelle-Calédonie, dénoncées et attribuées le 16 mai 2024 par le ministre de l'intérieur et des Outre-mer. Dans la foulée, le 17 mai, le SGDSN publiait une fiche technique réalisée par Viginum sur ces opérations pour appuyer les propos du ministre sur le volet informationnel.

Dans la même logique de compétence sectorielle, en prévision des élections européennes du 9 juin 2024, **le ministre délégué chargé de l'Europe Jean-Noël Barrot a alerté le 24 avril 2024 sur le risque de campagnes massives de désinformation et de déstabilisation.** Si cette prise de parole n'a pas été suivie d'une communication plus détaillée ou de l'attribution formelle d'une campagne numérique informationnelle, deux opérations ont néanmoins été révélées par d'autres canaux.

D'une part, la tête de liste Parti socialiste-Place publique Raphaël Glucksmann, **a indiqué à la presse le 16 avril 2024 avoir été averti du déroulement d'une opération de désinformation visant sa campagne. Cette manœuvre,** conduite par un réseau de comptes liés à la Chine, visait à présenter le candidat comme un « *cheval de Troie* » des États-Unis en Europe.

D'autre part, le journal Médiapart a révélé le 14 juin 2024 **une opération informationnelle visant à soutenir la campagne de la liste Rassemblement national menée par Jordan Bardella.** Cette opération, conduite par un réseau de comptes prorusses, a été portée par le SGDSN à la connaissance du candidat qui n'a pas souhaité la rendre publique selon le journal².

B. LA RÉPRESSION PÉNALE DES OPÉRATIONS D'INFLUENCE

1. En l'état du droit, une forte pluralité d'infractions à la disposition de l'autorité judiciaire pour réprimer les actes d'ingérence à visée d'influence

Compte tenu du caractère protéiforme des opérations d'influence, les services de l'État, en premier lieu les services de renseignement, peuvent

¹ Ministère de l'Europe et des affaires étrangères, [Ingérences numériques étrangères – Suite des investigations sur le réseau russe de propagande « Portal Kombat »](#), 15 février 2024.

² Mediapart, [« Des réseaux d'influence prorusses ont soutenu Jordan Bardella pendant la campagne des européennes »](#), 14 juin 2024, en ligne, consulté le 6 juillet 2024.

judiciariser les actions d'ingérence à visée d'influence sur une diversité de fondements.

a) Les atteintes aux intérêts fondamentaux de la Nation

Une opération d'ingérence à visée d'influence peut donner lieu à une qualification relevant des atteintes aux intérêts fondamentaux de la Nation (IFN). Ces derniers sont définis par le code pénal à son article 410-1 comme « *son indépendance, l'intégrité de son territoire, sa sécurité, la forme républicaine des institutions, les moyens de sa défense et de sa diplomatie, la sauvegarde de sa population en France et à l'étranger, l'équilibre de son milieu naturel et de son environnement et les éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel* ». **Au-delà d'intérêts purement régaliens, il importe de noter que les IFN comprennent de surcroît les intérêts économiques, scientifiques et culturels de la Nation.**

Le titre I^{er} du livre IV du code pénal définit et réprime les différentes atteintes aux IFN qui peuvent être classées en trois grandes catégories.

Premièrement, les atteintes aux IFN comprennent la trahison et l'espionnage¹. La distinction entre trahison et espionnage repose sur la nationalité de l'auteur. L'infraction est qualifiée de trahison lorsque l'auteur est français et d'espionnage lorsqu'il est de nationalité étrangère. **Ces infractions comprennent plusieurs comportements de nature délictuelle ou criminelle, notamment :**

- la livraison de tout ou partie du territoire national, de forces armées ou de matériel à une puissance étrangère (articles 411-2 à 411-3 du code pénal) ;
- les intelligences avec une puissance étrangère (articles 411-4 à 411-5 du code pénal) ;
- la livraison d'informations à une puissance étrangère (articles 411-6 à 411-8 du même code) ;
- le sabotage (article 411-9 du même code) ;
- la fourniture de fausses informations de nature à semer le trouble au sein du pays et à compromettre sa stabilité ou sa sécurité (article 411-10 du même code) ;
- la provocation aux crimes de trahison et d'espionnage (article 411-11 du même code).

Hormis l'infraction d'intelligence avec une puissance étrangère, ces infractions **ont en commun l'*animus hostilis*, un dol spécial imposant de caractériser que ces actes aient été commis en vue de servir les intérêts d'une puissance étrangère** au détriment des intérêts fondamentaux de la Nation et de l'Otan.

¹ Articles 411-1 à 411-11 du code pénal.

Deuxièmement, les dommages causés à la sécurité nationale sont inclus dans les atteintes aux intérêts fondamentaux de la Nation. Elles regroupent les infractions d'atteinte au secret de la défense nationale, les infractions d'atteinte à la sécurité des forces armées et aux zones protégées intéressant la défense nationale¹.

Une attention plus particulière doit être apportée aux intrusions dans des lieux protégés tels que les zones à régime restrictif (ZRR). Les établissements de recherche sont en effet particulièrement ciblés par les opérations d'influence malveillantes, justifiant l'intervention du réseau interministériel de protection du potentiel scientifique et technique de la Nation (PPST). L'entrée non autorisée dans des ZRR, tels que les laboratoires de recherche ou les lieux de production stratégique à protéger du fait de l'intérêt qu'elles présentent pour la compétitivité de l'établissement ou de la Nation est ainsi punie de six mois d'emprisonnement et de 7 500 euros d'amende².

Troisièmement, les atteintes aux IFN intègrent également d'autres atteintes aux institutions de la République ou à l'intégrité du territoire national, telles que l'attentat, le complot, ou le mouvement insurrectionnel³.

Au total, l'échelle des peines encourues pour les atteintes aux intérêts fondamentaux de la Nation va de sept ans d'emprisonnement et 100 000 euros d'amende à la détention criminelle à perpétuité et 750 000 euros d'amende, selon les infractions et les circonstances de leur commission.

b) Les infractions spécifiques relevant de la cybercriminalité

Les opérations d'influence intervenant très largement dans le domaine numérique, les infractions relevant de la cybercriminalité peuvent être utilement mobilisées.

En premier lieu, le champ des opérations d'ingérence à visée d'influence comprend les cyberattaques, en particulier lorsqu'elles sont associées à des manœuvres informationnelles. Ces attaques cyber peuvent faire l'objet :

- d'une qualification d'atteinte à un système de traitement automatisé de données (ASTAD), au titre des articles 323-1 à 323-4 du code pénal, notamment au moyen d'un rançongiciel ou dans le but d'opérer un déni de service ;

- d'une qualification de cyber sabotage (article 411-9 du même code), une aggravation étant prévue lorsqu'il est commis dans le but de servir une entité étrangère.

¹ Articles 413-1 à 413-7 du code pénal.

² Article 413-7 du code pénal.

³ Articles 412-1 à 412-8 du code pénal.

En second lieu, les opérations informationnelles en ligne à l'initiative d'une entité étrangère peuvent conduire à la diffusion amplifiée de messages haineux ou de contenus illicites. Ces comportements peuvent être appréhendés soit par le droit de la presse, soit par les infractions prévues par le code pénal.

S'agissant du droit de la presse, la loi du 29 juillet 1881 sur la liberté de la presse prévoit une série de délits et de crimes commis par voie de presse ou par tout autre moyen de publication pouvant permettre de réprimer une opération d'ingérence à visée d'influence, en particulier :

- les délits de diffamation et d'injures publiques (article 29 de la loi de 1881) qui peuvent faire l'objet d'aggravation de peines ;

- la provocation publique à la discrimination, à la haine ou à la violence raciale ou religieuse (article 24 alinéa 7 de la loi de 1881) et la provocation à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou identité de genre ou de leur handicap ou au discriminations prévues par les articles 225-2 et 432-7 du code pénal (article 24 alinéa 8 de la loi de 1881) ;

- l'apologie des crimes de guerre, des crimes contre l'humanité, des crimes ou délits de collaboration avec l'ennemi et des crimes de réduction en esclavage ou d'exploitation d'une personne réduite en esclavage, y compris si ces crimes n'ont pas donné lieu à la condamnation de leurs auteurs (article 24 alinéa 5 de la loi de 1881).

Certaines opérations d'influence étrangères menées en ligne peuvent impliquer la commission d'inflation sanctionnées par le code pénal, telles que :

- l'apologie du terrorisme, soit le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes (article 421-2-5 du code pénal) ;

- le cyberharcèlement (article 222-33-2-2 du même code) ;

- les faits de « doxxing », correspondant aux faits de divulgation malveillante de données personnelles, sont réprimées par l'article 223-1-1 du code pénal, une aggravation étant prévue lorsque cette divulgation touche les personnes dépositaires de l'autorité publique, chargées d'une mission de service public, titulaire d'un mandat électif public, candidates à un mandat électif public pendant la campagne ou journalistes.

La récente loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique a permis de compléter le droit en vigueur au regard des dernières évolutions technologiques et à la diffusion de fausses informations via des montages ou hypertrucages (*deep fakes*). Elle a ainsi :

- complété le délit de montage illicite prévu par l'article 226-8 du code pénal. Ce délit réprime en effet le fait de « publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son

consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention ». L'article 14 de la loi du 21 mai 2024 permet désormais d'assimiler à cette infraction « le fait de porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, un contenu visuel ou sonore généré par un traitement algorithmique et représentant l'image ou les paroles d'une personne, sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un contenu généré algorithmiquement ou s'il n'en est pas expressément fait mention ».

- créé une nouvelle infraction pour réprimer les montages à caractère sexuel (article 226-8-1 du code pénal).

Compte tenu de la multiplication des opérations d'influence impliquant des hypertrucages et visant tout particulièrement responsables publics et journalistes, **ces infractions devraient davantage être mobilisées à l'avenir.**

c) Les infractions spécifiques relevant du contentieux économique et financier

S'agissant du champ économique et industriel, **les actions d'ingérence à visée d'influence peuvent être appréhendées, au-delà des atteintes aux IFN, au moyen de qualifications de droit commun.** Il s'agit notamment du vol (article 311-1 du code pénal), du recel de délit (article 321-1 du code pénal), de l'abus de confiance (article 314-1 du code pénal), de la violation d'une obligation de confidentialité au titre du secret professionnel (article 226-13 du code pénal), de la divulgation illicite d'un secret de fabrique (article L. 621-1 du code de la propriété intellectuelle et article L. 1227-1 du code du travail) ou des atteintes aux systèmes de traitement automatisé de données.

Concernant les hypothèses de capture des élites, **l'autorité judiciaire peut mobiliser les infractions relevant des atteintes à la probité, en particulier les multiples infractions de corruption, dont :**

- la corruption active d'agent public (article 433-1 du code pénal), punie de 10 ans d'emprisonnement et d'une amende de 1 000 000 euros dont le montant peut être porté au double du produit tiré de l'infraction ;

- la corruption passive d'agent public (article 432-11 alinéa 1, 1° du même code) et **le trafic d'influence** (article 432-11 alinéa 1, 1° du même code). Ces infractions visent à punir l'agent public qui a accepté ou sollicité des offres, des promesses, des dons, des présents ou des avantages quelconques, soit, dans le premier cas, « pour accomplir ou avoir accompli, pour s'abstenir ou s'être abstenue d'accomplir un acte de sa fonction » ou, dans le second cas, « pour abuser ou avoir abusé de son influence réelle ou supposée en vue de faire obtenir d'une autorité ou d'une administration publique des distinctions, des emplois, des marchés ou toute autre décision favorable » ;

- la prise illégale d'intérêts (article 432-12 du même code), soit le fait pour « par une personne dépositaire de l'autorité publique ou chargée d'une mission

de service public ou par une personne investie d'un mandat électif public, de prendre, recevoir ou conserver, directement ou indirectement, un intérêt de nature à compromettre son impartialité, son indépendance ou son objectivité dans une entreprise ou dans une opération dont elle a, au moment de l'acte, en tout ou partie, la charge d'assurer la surveillance, l'administration, la liquidation ou le paiement ».

d) Les infractions spécifiques relevant du droit électoral

Les opérations d'ingérence à visée d'influence ciblent particulièrement les processus électoraux. À ce titre, le chapitre VII du titre premier du livre premier du code électoral précise les infractions en matière électorale.

D'une part, le droit électoral encadre strictement les modalités de financement des campagnes électorales et des groupes politiques. Il réprime notamment les faits tendant à influencer le vote d'un ou plusieurs électeurs (articles L. 106 à 108 du code électoral), par des dons ou libéralités ou par des voies de fait, violences ou menaces.

De plus, le régime du financement des campagnes électorales, en application des articles L 52-8 et L 113-1 du code électoral, punit :

- l'octroi de prêts par les personnes physiques étrangères ou ne résidant pas en France ;

- les dons ou fournitures de biens, services ou autres avantages directs ou indirects, à des prix inférieurs à ceux qui sont habituellement pratiqués, par des personnes morales ;

- l'octroi de prêts ou la fourniture de garantie pour des prêts par des personnes morales, à l'exception des partis et groupements politiques ainsi que des établissements de crédit ou sociétés de financement ayant leur siège social dans un État membre de l'Union européenne ou partie à l'accord sur l'Espace économique européen ;

Au titre de l'article 11-5 de la loi n° 88-227 du 11 mars 1988 relative à la transparence financière de la vie politique, **sont prévues les infractions suivantes au financement des groupements politiques :**

- l'interdiction de don à un parti ou groupement politique pour les personnes physiques qui ne sont pas de nationalité française ou ne résidant pas en France ;

- les dons ou fournitures de biens, services ou autres avantages directs ou indirects, à des prix inférieurs à ceux qui sont habituellement pratiqués, par des personnes morales ;

- l'interdiction de financement d'un parti ou groupement politique français par un État étranger ou une personne morale de droit étranger, à l'exception des partis et groupements politiques ainsi que des établissements de crédit et sociétés de financement ayant leur siège social dans un État membre de l'UE ou partie à l'accord sur l'Espace économique européen.

D'autre part, les opérations d'ingérences informationnelles peuvent notamment concerter des atteintes portées à la sérénité et à la sincérité du scrutin et notamment la diffusion de fausses nouvelles ou fraudes en vue d'influer sur le vote. À cet égard, l'article L. 97 du code électoral dispose que ceux qui « à l'aide de fausses nouvelles, bruits calomnieux ou autres manœuvres frauduleuses, auront surpris ou détourné des suffrages, déterminé un ou plusieurs électeurs à s'abstenir de voter, seront punis d'un emprisonnement d'un an et d'une amende de 15 000 euros ».

e) Les infractions de droit commun

Dans un contexte de multiplication des opérations d'influence malveillante sur le sol français, dans une dynamique de « *clandestinisation* » des actions d'influence, **les infractions de droit commun peuvent être mobilisées.**

La direction des affaires criminelles et des grâces a ainsi indiqué à la commission d'enquête **qu'il a pu être recouru à plusieurs types de qualifications pénales au cours des derniers mois, dont :**

- les violences aggravées (articles 222-11 à 222-13 du code pénal) ;
- les destructions ou dégradations aggravées notamment lorsqu'elles sont commises en réunion, à l'encontre d'un lieu classifié au titre du secret de la défense nationale, d'une part ou au préjudice d'un magistrat, d'un juré, d'un avocat, d'un officier public ou ministériel, d'un militaire de la gendarmerie, d'un fonctionnaire de la police nationale, des douanes, de l'administration pénitentiaire ou de toute autre personne dépositaire de l'autorité publique ou chargée d'une mission de service public, en vue d'influencer son comportement dans l'exercice de ses fonctions ou de sa mission, d'autre part (articles 322-3 à 322-4 du code pénal) ou encore aggravées à raison de l'appartenance ou la non appartenance d'une victime ou d'un groupe de personnes dont fait partie la victime à une prétendue race, une ethnie, une nation ou une religion déterminée (article 132-76 du code pénal) ;
- les destructions, dégradations et détériorations dangereuses pour les personnes (articles 322-5 à 322-11-1) ;
- la participation à une association de malfaiteurs en vue de commettre un crime ou un délit puni de 5 ans ou 10 ans d'emprisonnement (article 450-1 du code pénal) ;
- la participation à un groupement en vue de la préparation de violences volontaires ou de dégradations de biens (article 222-14-2 du même code).

À titre d'exemple, **l'infraction de dégradation aggravée** à raison de l'appartenance ou la non appartenance d'une victime ou d'un groupe de personnes dont fait partie la victime à une prétendue race, une ethnie, une

nation ou une religion déterminée a été mobilisée par le parquet de Paris **dans l'affaire dite des étoiles de David**.

2. Un arsenal pénal récemment renforcé par l'adoption de la proposition de loi visant à prévenir les ingérences étrangères en France

a) La création d'une circonstance aggravante d'ingérence étrangère et l'autorisation du recours aux techniques spéciales d'enquête

Dans le prolongement des travaux de la délégation parlementaire au renseignement, le président de la commission des lois de l'Assemblée nationale, M. Sacha Houlié a déposé le 6 février 2024 **une proposition de loi visant à prévenir les ingérences étrangères en France**. Ce texte, définitivement adopté par l'Assemblée le 5 juin 2024, a introduit à l'initiative de la rapporteure de la commission des lois du Sénat, Mme Agnès Canayer, deux dispositifs visant à renforcer l'arsenal pénal pour entraver les opérations d'ingérences.

En premier lieu, l'article 8 de la proposition de loi crée une **circonstance aggravante** applicable aux infractions contre les biens ou les personnes conduites dans le but de servir les intérêts d'une puissance étrangère ou d'une entreprise ou d'une organisation étrangère ou sous contrôle étranger. L'alourdissement des peines encourues devrait contribuer à renforcer l'efficacité de l'entrave aux actions d'ingérence à visée d'influence.

Le champ des infractions concernées par cette nouvelle circonstance aggravante est particulièrement large puisqu'il intègre l'ensemble des atteintes à la personne humaine¹ et une majeure partie des crimes et délits contre les biens², permettant une réponse complète aux ingérences. Si les atteintes aux intérêts fondamentaux de la Nation ne sont pas couvertes par cette circonstance aggravante, ses éléments constitutifs peuvent déjà inclus dans l'infraction, comme pour l'intelligence avec une puissance étrangère, ou lorsqu'une circonstance aggravante similaire est déjà prévue comme pour le sabotage.

L'affaire des étoiles de David constitue un exemple topique d'opération d'ingérence à visé d'influence face à laquelle l'autorité judiciaire pourrait mobiliser la nouvelle circonstance aggravante. Une action de ce type, intervenue après l'entrée en vigueur de la loi visant à prévenir les ingérences étrangères en France, rentreraient en effet dans le champ d'application de la proposition de loi.

En second lieu, l'article 8 de la loi « Ingérences étrangères » permet le recours aux techniques spéciales d'enquête dans les affaires d'ingérence étrangère. Ces techniques, jusqu'ici réservées à la criminalité et à la

¹ Titre II du livre II du code pénal.

² Titre Ier et chapitres II et III du titre II du livre III du code pénal.

délinquance organisées et aux crimes (article 706-73 du code de procédure pénale), comprennent notamment le recueil des données techniques de connexion et les interceptions de correspondances émises par la voie des communications électroniques, les sonorisations et les fixations d'images de certains lieux ou véhicules ou la captation des données informatiques.

b) Une réduction de la dispersion des compétences juridictionnelles par l'instauration d'une compétence concurrente au profit des juridictions parisiennes pour connaître des infractions aggravées de la circonference d'ingérence étrangère

Le caractère disparate du corpus infractionnel applicable aux actes d'ingérence à visée d'influence conduit à l'intervention d'une pluralité de juridictions. **Ceci s'explique par l'application des critères de compétence territoriale et des critères de compétence relatifs à la spécificité des contentieux.**

Aussi, s'agissant des atteintes aux intérêts fondamentaux de la Nation, les juridictions compétentes diffèrent selon que l'on se trouve en temps de guerre ou en temps de paix, sur le sol français ou à l'étranger ou la qualité de militaire ou non de l'auteur. Parmi les juridictions compétentes, on peut citer :

- **les neuf juridictions de droit commun spécialisées en matière militaire**¹ compétentes pour connaître des infractions commises sur le territoire de la République par un militaire agissant dans l'exercice du service (article 697-1 du code de procédure pénale) et des infractions de trahison, espionnage et compromission commises par toute autre personne sur le territoire de la République (article 702 du code de procédure pénale) ;

- **le tribunal judiciaire de Paris**, compétent concurremment pour connaître des infractions de trahison, espionnage et compromission commises sur le territoire de la République ou à l'étranger ;

- **la juridiction de droit commun spécialisée en matière militaire de Paris**, qui dispose d'une compétence exclusive pour connaître des infractions commises hors du territoire de la République par les militaires agissant dans l'exercice du service (article 697-4 du code de procédure pénale).

Concernant la cybercriminalité, toutes les juridictions peuvent connaître de faits de cybercriminalité. **Pour autant, des compétences spéciales ont été instituées en vue de leur traitement spécialisé.**

Ainsi, **la juridiction parisienne dispose d'une compétence nationale concurrente en matière d'atteinte aux systèmes de traitement automatisé, depuis la loi n° 2016-731 du 3 juin 2016**². Dans le même sens, la section « cyber » du parquet de Paris (J3) a été intégrée à la Juridiction nationale

¹ Dont la liste est fixée par le décret n° 2014-1443 du 3 décembre 2014.

² Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

chargée de la lutte contre la criminalité organisée (Junalco). Pour clarifier les règles de compétences entre les juridictions locales, les juridictions inter-régionales spécialisées (JIRS) et le tribunal judiciaire de Paris, une dépêche du Garde des sceaux du 9 juin 2021 a établi des critères de répartition des affaires selon leur degré de complexité et leur nature.

De plus, en matière de lutte contre la diffusion des contenus haineux, **une circulaire du 24 novembre 2020 a créé à droit constant un pôle national de lutte contre la haine en ligne et a désigné le tribunal judiciaire de Paris comme échelon adéquat pour centraliser, sous la direction du procureur de Paris, le traitement des affaires significatives de cyberharcèlement et de haine en ligne.**

La loi « Ingérences étrangères » **tend à clarifier cette répartition en instaurant une compétence concurrente au profit des juridictions parisiennes** pour connaître des infractions aggravées de la circonstance d'ingérence étrangère. En effet, le nouveau texte a introduit :

- une compétence des neuf juridictions spécialisées en matière d'atteints aux IFN ainsi qu'une compétence concurrence du parquet, du tribunal judiciaire et de la cour d'assises de Paris pour connaître des infractions aggravées par la nouvelle circonstance aggravante ;

- une compétence concurrente de la section cyber du parquet de Paris, lorsque les infractions constitutives d'un acte d'ingérence étrangère sont des atteintes aux systèmes de traitement automatisés des données.

Néanmoins, comme le relève la direction des affaires criminelles et des grâces (DAGC) du ministère de la justice, en pratique, les affaires d'ingérences sont essentiellement traitées par le tribunal judiciaire de Paris.

En outre, pour pallier cette pluralité de juridictions, **une information des juridictions sur les infractions mobilisables et les acteurs compétents est assurée par la DAGC**. Au mois de juin 2021, la DAGC a transmis à l'ensemble des magistrats un « DAGC Focus » dédiée à la lutte contre les ingérences étrangères qui a fait l'objet d'une actualisation en avril 2024 et que la commission d'enquête s'est procuré. Il devrait être de nouveau révisé à la suite de la publication de la loi « Ingérences étrangères ».

c) *Vers une meilleure judiciarisation des opérations d'ingérence à visée d'influence ?*

La judiciarisation des opérations d'ingérence à visée d'influence est cependant complexe. C'est particulièrement le cas s'agissant des manœuvres informationnelles, comme le relève l'Ambassadrice pour la diplomatie publique en Afrique, Anne-Sophie Avé : « *pour judiciariser, il faut des preuves et, dans un État de droit, c'est bien normal. En la matière, on ne peut agir que sur la*

base de la diffamation, de l'injure publique ou de l'incitation à la haine, et encore faut-il que ces éléments soient constitués dans une publication »¹.

Outre ces difficultés de caractérisation juridique, **l'engagement de poursuites pénales soulève une difficulté d'opportunité**, rappelée par le rapport de la délégation parlementaire au renseignement dans son rapport d'activité pour l'année 2022-2023². Le risque d'un échec des poursuites **expose les services de l'État à la révélation de ses sources et des modes opératoires** des services de renseignement. Entre 2019 et 2023, **moins de cinq personnes par an ont été mises en cause pour les infractions d'espionnage ou de trahison**, seule l'année 2020 ayant donné lieu à des condamnations.

L'entrée en vigueur de la loi visant à prévenir les ingérences étrangères devrait contribuer à améliorer la judiciarisation des affaires. Les techniques spéciales d'enquête, similaires aux moyens dont pourront disposer les services de renseignement, devraient permettre de faciliter la recherche de la preuve. De plus, **ce recours aux techniques spéciales permet d'éviter une discontinuité dans les méthodes utilisées à compter de la judiciarisation.** Jusqu'à maintenant, l'autorité judiciaire se trouvait en effet démunie par rapport aux capacités des services de renseignement pour enquêter sur ce type d'affaires.

Combiné avec l'intervention de services de police judiciaire spécialisés comme la direction générale de la sécurité intérieure, **l'usage des techniques spéciales d'enquête devrait ainsi faciliter l'établissement de la preuve.**

En tout état de cause, compte tenu du fait que les ingérences à visée d'influence relèvent essentiellement du champ des services de renseignement, **il apparaît indispensable d'assurer une bonne coordination entre l'autorité judiciaire et les autres services de l'État luttant contre les opérations d'influence.** La DACG échange ainsi régulièrement avec la DGSI et le SGDSN. D'une part, ces services **informent le ministère de la justice de l'évolution de la menace pour mieux appréhender les phénomènes d'ingérences sur le plan judiciaire.** La directrice générale de la sécurité intérieure, Céline Berthon souligne ainsi que « *l'autorité judiciaire doit également être accompagnée afin qu'elle puisse prendre en compte ces problématiques spécifiques d'espionnage économique ou industriel – des infractions qui ne sont pas les plus couramment poursuivies par cette autorité* »³. D'autre part, **ils travaillent à articuler la réponse judiciaire au sein de la palette d'entraves à la disposition des services de l'État.**

Ces efforts de coordination sont encore renforcés en matière de cybercriminalité. Suite au Conseil de défense cyber du 1^{er} avril 2019, une

¹ [Audition](#) du 30 avril 2024.

² [Rapport public n° 1454 \(seizième législature- Assemblée nationale\) / n° 810 \(2022-2023 – Sénat\)](#) fait par Sacha Houlié au nom de la délégation parlementaire au renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023, déposé le 29 juin 2023.

³ [Audition](#) du 21 mars 2024 (à huis clos).

comitologie spécifique a été créée sous l'égide du SGDSN pour coordonner les réponses administratives, judiciaires et diplomatiques aux menaces cyber et informationnelles. Une **formation spéciale du C4, le C4STRAT-Jud associe par conséquent le parquet de Paris**, notamment la Junalco, et la DACG. Cette formation, qui se réunit tous les semestres, **permet à l'ensemble des services de mieux appréhender les enjeux de judiciarisation**. De plus, au sein du C4STRAT-Jud, les services du ministère de la justice travaillent plus spécifiquement avec Viginum pour approfondir les questions de manipulations de l'information.

C. LA POLITIQUE D'INFLUENCE POSITIVE : MAILLON FAIBLE DE LA RÉPONSE FRANÇAISE

1. La France pâtit de l'absence d'une véritable politique d'influence

En miroir d'une politique d'influence défensive, visant en premier lieu à répondre aux actions d'influence malveillantes menées par des États compétiteurs, **il paraît indispensable de disposer d'une politique d'influence plus offensive**. Aux côtés de capacités à contrer les attaques, en particulier sur le plan informationnel, **une puissance comme la France doit disposer de moyens de promotion de ses valeurs, de son action et de sa vision du monde sur la scène internationale**. Dans un contexte de lutte contre les opérations d'influence malveillantes, une telle politique **permet d'offrir un modèle alternatif aux principes mis en œuvre par les régimes autoritaires et illibéraux** et d'affaiblir les fondements de la désinformation. Pour l'Ambassadrice pour la diplomatie publique, Anne-Sophie Avé : « *Poser un narratif positif, c'est le plus important, et l'on n'en est pas encore là* »¹.

Toutefois, force est de constater qu'en matière d'influence, l'action extérieure de la France ne semble pas disposer d'une vision politique unifiée, d'un « narratif » sur lequel s'appuyer. Pour Frédéric Charillon : « *Aucune doctrine, peu de cadres autres que quelques points de repère ne viennent définir la diplomatie d'influence à la française. Celle-ci reste une pratique ad hoc, comme un objectif implicite assigné à l'ensemble des services, mais qui ne saurait constituer le monopole d'aucune direction ou d'aucun acteur. On classe sous le terme "politique d'influence" des ambitions variables, qui vont de l'entretien de l'image de la France jusqu'au ralliement de soutiens étatiques (ou de votes dans les organisations internationales) en faveur de ses initiatives politiques, en passant par la présence française dans les lieux de production d'idées, la promotion des entreprises françaises ou d'un contexte économique national favorable à l'investissement* »².

L'architecture du programme n° 185 « diplomatie culturelle et d'influence », de la mission budgétaire « Action extérieure de l'État », traduit

¹ [Audition](#) du 30 avril 2024.

² Frédéric Charillon, « Chapitre IV. Les politiques d'influence », in Maurice Vaisse éd., *Diplomatie française. Outils et acteurs depuis 1980*, Odile Jacob, 2018.

la complexité à articuler dans une même politique publique d'influence des actions différentes. Le programme n° 185 regroupe en effet les actions du ministère de l'Europe et des affaires étrangères tant en matière de promotion de la francophonie, que d'attractivité universitaire, d'attractivité économique ou de coopération culturelle. À ce programme spécifique s'ajoute les crédits de la mission « Aide publique au développement » qui contribuent très largement à l'influence de la France à l'étranger.

La disproportion des moyens financiers accordés à nos instruments d'influence pèse également sur l'efficacité de cette politique. L'exemple de l'audiovisuel extérieur est frappant. Le groupe France Médias Monde (FMM) qui regroupe la chaîne d'information France 24, la radio mondiale RFI, et la radio en langue arabe Monte Carlo Doualiya, dispose d'une dotation publique de 275,3 millions d'euros en 2024. **Par comparaison, les médias internationaux de nos partenaires sont largement mieux dotés** avec 412 millions d'euros de budget pour *BBC World Service*, 408 millions d'euros pour *Deutsche Welle* et 820 millions d'euros pour *USA Global Media*. **Il en va de même pour les audiovisuels extérieurs des États qui ne partagent pas nos valeurs** puisque RT et Sputnik disposaient ensemble d'un budget de 430 millions d'euros en 2022.

Pour autant et au-delà de ses fragilités structurelles évoquées plus haut (voir *Première partie, III*), la France dispose d'atouts considérables dans la compétition d'influences à l'échelle internationale.

2. En dépit d'efforts sectoriels, la France peine à faire émerger une politique d'influence *ex nihilo*

Une politique d'influence ne se décrète pas. La Gouvernement a tenté, depuis 2017, de faire émerger une véritable politique d'influence, au-delà d'une accumulation de politiques sectorielles. Toutefois, **les tâtonnements du ministère de l'Europe et des affaires étrangères et les résultats limités obtenus illustrent la difficulté à faire émerger une politique d'influence positive cohérente à partir d'actions dont la coordination n'a rien d'évidente.**

Le ministère de l'Europe et des affaires étrangères a publié en 2021 une « *Feuille de route de l'influence* » visant à recenser l'ensemble des leviers d'influence existant au sein de l'action extérieure de l'État et à recenser des leviers opérationnels de consolidation d'une politique d'influence. Cependant, au-delà d'un utile inventaire de nos leviers d'influence, **les outils avancés par cette feuille de route pour coordonner et consolider l'action du ministère en matière d'influence, loin de constituer une politique publique, ont fait long feu.** Parmi les outils avancés figurait notamment un « *tableau de bord de l'influence* » visant à agréger « *des données chiffrées relatives à toutes les politiques d'influence, ce tableau de bord [et à permettre] de présenter une photographie de la performance d'influence de la France, dans les secteurs stratégiques*

pertinents ». Par manque d'opérationnalité ou de volontarisme, cette proposition n'a pas été traduite dans les faits. Le directeur général de la mondialisation, Aurélien Lechevallier¹, auditionné par le rapporteur, a confirmé que ce tableau de bord de l'influence n'avait jamais été mis en œuvre.

La volonté de placer l'influence au centre de l'action du MEAE s'est également traduite dans son organisation interne, avec peu de succès, comme l'a rappelé l'Ambassadeur pour le numérique Henri Verdier : « *La direction des affaires culturelles a été rebaptisée "diplomatie d'influence", mais elle va retrouver son intitulé d'origine, car il n'est pas facile pour un diplomate de dire : "Bonjour, je viens vous influencer". Promouvoir notre culture, nos artistes, la langue française, la coopération internationale – on y met beaucoup d'argent – est une forme d'influence* »². En 2023, la direction de la diplomatie d'influence est redevenue la direction de la diplomatie culturelle, audiovisuelle, éducative, universitaire et scientifique³.

Dans une approche plus interministérielle, la Revue nationale stratégique (RNS) de 2023 a consacré l'influence comme une nouvelle fonction stratégique, tout en soulignant son caractère transversal et l'inévitable coordination qu'elle implique : « *L'influence, dans toutes ses dimensions – diplomatique, militaire, économique, culturelle, sportive, linguistique, informationnelle – est un domaine de contestation, qui nous impose une réponse coordonnée. Elle constitue une nouvelle fonction stratégique à part entière* »⁴.

À l'occasion de son discours de clôture des États généraux de la diplomatie, le président de la République a confirmé le chef de filât du ministère de l'Europe et des affaires étrangères sur la fonction d'influence : « *nous devons organiser notre capacité d'influence, et le ministère des Affaires étrangères en est la cheville ouvrière pour l'international* »⁵. À cet égard, le rapport rendu à la ministre de l'Europe et des affaires étrangères dans le cadre de ces États généraux avait qualifié le MEAE de « *ministère de l'influence en Europe et dans le monde* »⁶.

L'élaboration d'une Stratégie nationale d'influence (SNI), prévue par la Revue nationale stratégique et préparée par le Quai d'Orsay a permis de préciser le cadre d'intervention de la politique d'influence de la France. La commission d'enquête a eu communication ce document non public.

D'une part, il en ressort que la SNI établit clairement des limites à l'action d'influence de la France, en raison de « *son héritage historique, par les*

¹ Audition du rapporteur, 18 juin 2024.

² [Audition](#) du 28 mars 2024.

³ Décret n° 2023-1335 du 29 décembre 2023 modifiant le décret n° 2012-1511 du 28 décembre 2012 portant organisation de l'administration centrale du ministère des affaires étrangères.

⁴ Secrétariat général de la défense et de la sécurité nationale, [Revue nationale stratégique 2022](#).

⁵ [Discours du président de la République Emmanuel Macron à l'occasion de la clôture des États généraux de la diplomatie](#), 16 mars 2023.

⁶ Ministère de l'Europe et des affaires étrangères, [« Pour un plan de réarmement de la diplomatie française »](#), mars 2023.

fondements de son organisation politique et institutionnelle, par les traités dont elle est signataire ». Par conséquent, **la politique d'influence française ne peut être qu'« affirmative » et porter ses valeurs et ses intérêts sans agressivité**. La France exclut donc clairement de recourir aux mêmes outils d'influence malveillante que certains États dont « *la désinformation, la manipulation, l'industrie du mensonge* ». Le ministre de l'Europe et des affaires étrangères l'a ainsi souligné devant la commission d'enquête : « *La France ne fait pas d'ingérence ; elle fait de l'influence, de manière transparente et dans un cadre démocratique, pour aider nos entreprises à gagner des parts de marché, pour défendre ses valeurs universalistes et ses intérêts aux niveaux bilatéral et multilatéral, dans les organisations internationales, comme le G7 ou l'Union européenne* »¹.

D'autre part, cette nouvelle stratégie fixe de grands objectifs à notre politique d'influence à savoir :

- **à court terme**, favoriser un « *environnement de perceptions propice à nos politique et nos initiatives* » ;
- **à moyen terme**, renforcer l'image de la France dans le monde à la suite d'une analyse de ses atouts et de ses vulnérabilités en assumant un rôle de puissance d'équilibre ;
- **à plus long terme**, renforcer l'attractivité de la France et son rayonnement dans tous les domaines.

Pour autant, au-delà de ces objectifs très larges, la SNI peine à sortir d'un effet d'inventaire, listant les domaines dans lesquels la France doit renforcer son influence, sans parvenir à faire émerger un « récit » du rôle qu'elle entend jouer dans le monde. Le directeur général de la mondialisation a **confirmé la difficulté à consolider l'ensemble de ces actions en une politique d'influence positif**. À cet égard, la commission d'enquête recommande de suivre avec attention les travaux du comité de suivi de la SNI, notamment chargé du décloisonnement de notre approche en matière d'influence.

Dans un contexte où la France entend se distinguer par une politique d'influence positive, associant la société civile et ses partenaires, dans le respect des principes démocratiques, **l'absence de publication de la stratégie nationale d'influence interroge**. Ce manque de transparence ne contribue pas à clarifier les objectifs de notre politique d'influence. Dans un environnement de compétition, voire de confrontation, imposé par des stratégies étatiques agressives, **il importe d'assurer la lisibilité de notre action extérieure**.

Hormis ce point, la structuration d'une politique française d'influence positive s'est sensiblement améliorée au cours des dernières années, au travers d'efforts sectoriels. **Sans balayer l'ensemble des actions diplomatiques de la France, ce qui excéderait largement l'objet de la commission d'enquête, deux exemples peuvent être soulignés**.

¹ [Audition](#) du 18 juin 2024.

En premier lieu, **le redressement de notre politique d'aide publique au développement, tant dans ses moyens que dans sa doctrine, contribue à renforcer de manière significative l'influence de la France**. La loi n° 2021-1031 du 4 août 2021 de programmation relative au développement solidaire et à la lutte contre les inégalités mondiales a ainsi fixé une trajectoire ascendante de l'APD pour atteindre 0,7 % du revenu national brut (RNB) en 2025. Le montant total de l'aide publique au développement (APD) a en effet plus que doublé entre 2017 et 2024. Ces volumes financiers, sans constituer un but en soi, constituent néanmoins un accélérateur d'influence. À titre d'exemple, en matière humanitaire, la progression considérable des contributions volontaires aux Nations unies (CVNU), passées de 7,5 millions d'euros en 2017 à 200 millions d'euros en 2024, ont permis à la France de regagner des parts d'influence au sein du système onusien.

En outre, la direction générale de la mondialisation, de la culture, de l'enseignement et du développement international, responsable au sein du MEAE pour la conduite de la politique de développement, **a accentué les actions de communication et de valorisation des efforts de la France en la matière**. Le Fonds de solidarité pour les projets innovants (FSPI), créé en 2016, illustre cette logique. Cet instrument, doté de 100 millions d'euros en 2024 et piloté par les ambassades, **vise à financer sur le terrain des « actions innovantes à impact rapide » et « fortement visibles »**. Il s'agit de petits projets, au coût inférieur à un million d'euros, et à fort impact communicationnel.

En second lieu, **le renforcement des moyens de communication du ministère de l'Europe et des affaires étrangères participe d'une promotion et d'une valorisation de l'action de la France à l'international**. Comme exposé *supra*, la montée en puissance de la communication du MEAE et en particulier la création, au sein de la direction de la communication et de la presse d'une sous-direction « veille et stratégie » a permis de renforcer le volet « offensif » de cette communication stratégique. Ce renforcement poursuit également l'objectif de **porter un discours plus positif et affirmatif, à même de promouvoir l'action de la France**. La direction de la communication et de la presse (DCP) anime en ce sens un réseau de 530 agents chargés de participer aux fonctions de communication, tous statuts et toutes fonctions confondues. Selon l'Ambassadrice pour la diplomatie publique en Afrique, Anne-Sophie Avé : « *Des gens sont prêts à croire n'importe quoi, qui plus est aujourd'hui, avec les réseaux sociaux : il faut réagir, il faut être présent dans les médias, car la nature a horreur du vide. Il faut détailler, humblement, le travail mené au quotidien, par exemple en accompagnant des chantiers de fouilles archéologiques ; dire que nous en sommes heureux, car de tels travaux nous apprennent quelque chose à nous, Français, de l'histoire de l'humanité ; ne pas laisser croire que nous nous contentons de financer* »¹.

¹ [Audition](#) du 30 avril 2024.

Cette stratégie de communication permet, à terme, de disposer de relais locaux pouvant porter un message positif sur la France. Sans recourir, comme certains États, à des *proxies* locaux rémunérés pour diffuser un discours de propagande et de désinformation, il s'agit de convaincre des relais d'opinion, par un récit positif de l'action française.

L'accent porté sur cette communication d'influence repose également sur des actions de formation, au sein de la nouvelle Académie diplomatique et consulaire.

D. LA COORDINATION EUROPÉENNE ET INTERNATIONALE : UNE RÉPONSE EN CONSTRUCTION FACE AUX STRATÉGIES D'INFLUENCE AGRESSIVES

1. En matière de communication stratégique et de dénonciation

a) Les initiatives des États : l'exemple de la mobilisation du format Weimar

En dehors des organisations internationales, les États peuvent organiser des coopérations renforcées en matière de lutte contre les opérations d'influence malveillante. Début 2024, la France s'est ainsi engagée, avec ses partenaires allemands et polonais, à mobiliser le format dit « de Weimar » dans la lutte contre les manipulations de l'information.

Le format trilatéral du triangle de Weimar a été initié en 1991 par le ministre allemand des affaires étrangères, Hans-Dietrich Genscher, avec ses homologues français, Roland Dumas, et polonais, Krzysztof Skubiszewski. Les objectifs initiaux de cette concertation se concentraient sur la réconciliation germano-polonaise et l'intégration de la Pologne dans l'Otan et l'Union européenne. Le format a ensuite évolué pour devenir une instance de concertation au sein de l'UE.

Progressivement tombé en désuétude du fait du positionnement du gouvernement polonais dominé par le parti Droit et Justice de 2015 à 2023, le triangle de Weimar a donc récemment été réactivé dans la lutte contre la désinformation.

Cette coordination plus forte entre trois grands États membres de l'Union s'est traduite à l'occasion de conférences de presse et déclarations communes depuis le début de l'année 2024. Sur un plan opérationnel, elle a donné lieu :

- à la **mise en place d'un programme d'alerte et de réaction** dans le cadre du Triangle de Weimar sur la manipulation de l'information ;

- à l'**engagement de création d'un fonds commun consacré au financement de projets** soutenant la résilience des médias à l'étranger.

Cette coopération trilatérale participe d'une prise de conscience collective sur la menace des opérations d'influence. Le ministre de l'Europe et

des affaires étrangères Stéphane Séjourné le soulignait ainsi : « *Il est bon que les Français sachent, par exemple, qu'une attaque massive d'ingérence a eu lieu hier en Pologne et en Allemagne : cela illustre l'ampleur de la menace pour toutes les démocraties européennes. À l'heure où la parole publique est mise en cause, cette communication montre la réalité du danger, participe de l'éducation de l'opinion* »¹. Les trois partenaires se sont engagés pour prononcer des dénonciations communes d'activités informationnelles malveillantes de la part de la Russie, dans un format Weimar. En février 2024, la dénonciation du réseau prorusse *Portal Kombat* a ainsi été opérée en amont d'un sommet tripartite.

DOCUMENT PROVISOIRE

¹ [Audition](#) du 18 juin 2024.

Portal Kombat

Le 12 février 2024, la France a mis au jour un vaste réseau de désinformation prorusse, « *Portal Kombat* ». Le service Viginum a enquêté en source ouverte sur ce réseau dont l'apparition remonterait à 2013 et reposant sur trois écosystèmes : « *pravda* », « *-news.ru* » et un ensemble de sites plus anciens¹.

Cette opération présente la caractéristique de ne produire aucun contenu original. Les sites du réseau relayaient ainsi des publications issues de trois sources principales : des comptes de personnalités prorusses, des agences de presse russes ou des sites d'institutions. Ces contenus faisaient l'objet d'une traduction automatique du russe vers la langue du pays visé. Sur un plan technique, l'opération reposait sur un travail de référencement optimisé sur les principaux moteurs de recherche, de sorte à augmenter la portée de diffusion de ses contenus. Cette diffusion était massivement amplifiée par des *bots* sur les réseaux sociaux. Une partie de cette amplification artificielle a reposé sur des comptes liés à la campagne *RRN/Doppelgänger*.

L'activité du réseau était initialement dirigée vers des audiences russes et ukrainiennes avec des sites spécialisées selon les localités concernées. À compter de l'invasion russe de l'Ukraine, l'opération s'est tournée vers une audience plus internationale et une diffusion de contenus favorables à l'*« opération militaire spéciale »* et dénigrant l'Ukraine et ses dirigeants. L'Allemagne, l'Autriche, les États-Unis, l'Espagne, la France, la Pologne, la Suisse et le Royaume-Uni ont ainsi été visés.

Cette redirection vers des pays hors des espaces russophones et ukrainophones s'est accompagnée d'un ciblage des contenus selon les pays. Dans le cas de la France, les narratifs propagés, au-delà d'une présentation positive de la Russie et d'une critique de l'Ukraine, reprenaient des thèses proches des sphères complotistes francophones. Les manœuvres informationnelles de *Portal Kombat* présentaient également un caractère opportuniste en traitant de sujets d'actualité internationale pouvant profiter au Kremlin.

Viginum a établi le rôle central d'une entreprise russe installée en Crimée, *TigerWeb*, dans la création et l'animation de l'écosystème *Portal Kombat*². Cette société, dirigée par Evgueni Chevtchenko, serait liée à *Infores*, agence de presse identifiée comme un paravent de l'unité 54777 du renseignement militaire russe (GRU), responsable des opérations psychologiques. Au total, le service Viginum a identifié 224 portails affiliés au réseau de l'opération *Portal Kombat*.

Source : commission d'enquête d'après Viginum

La France fait au demeurant partie des États membres les plus actifs pour renforcer les capacités communes européennes face aux *FIMI*. Lors de son audition devant la commission d'enquête, le ministre délégué chargé de l'Europe, Jean-Noël Barrot, a ainsi cité deux initiatives récentes en ce sens.

Premièrement, la France, conjointement avec ses partenaires du Triangle de Weimar, l'Allemagne et la Pologne, a fait devant le conseil affaires

¹ Viginum, « *Portal Kombat : un réseau structuré et coordonné de propagande prorusse* », Rapport technique, février 2024.

² Viginum, « *Portal Kombat : un réseau structuré et coordonné de propagande prorusse* », Second rapport technique, février 2024.

générales du 21 mai 2024 une déclaration commune appelant la Commission européenne à prendre 20 mesures destinées à mieux protéger la démocratie et le débat public, dont notamment :

- engager résolument le travail sur un nouveau régime de sanctions visant les opérations russes de manipulation de l'information ;
- donner une force obligatoire le Code européen de bonne conduite sur la lutte contre la désinformation sur les plateformes (voir *III*).

Le ministre a précisé que cette déclaration a été soutenue par 16 États membres.

En deuxième lieu, au niveau « paneuropéen », le ministre a indiqué que la France a plaidé pour que l'ordre du jour du sommet de la Communauté politique européenne du 18 juillet 2024, l'instance de dialogue créée à l'initiative de la France suite au déclenchement de la guerre en Ukraine, intègre les enjeux de « défense de la démocratie », parmi lesquels les opérations de désinformations menées par nos compétiteurs.¹

b) L'action du Service européen pour l'action extérieure : une forte concentration sur la désinformation russe

En complément du système d'alerte rapide (SAR) qui permet, au stade de la détection et de la caractérisation, un partage d'informations entre les États de l'Union, le service européen pour l'action extérieure (SEAE) comporte également une capacité de riposte. **Ont été créées au sein de la division de la communication stratégique du SEAE, trois task forces chargées de la lutte contre la désinformation :**

- **une task force chargée de la communication stratégique dans le voisinage oriental** (*East StratCom Task Force*), créée en septembre 2015 suite aux conclusions du Conseil européen des 19 et 20 mars 2015 soulignant la nécessité de « contrer les campagnes de désinformation de la Russie », et dotée d'une quinzaine d'agents ;
- **une task force chargée de la communication stratégique dans le voisinage méridional de l'UE et la région du Golfe** (*« South StratCom Task Force »*) créée en 2015 ;
- **une task force chargée de la communication stratégique pour les Balkans occidentaux**, créée en 2017.

Il est intéressant de noter que seule la *East StratCom Task Force* s'est vue confiée, dès sa création, un mandat de lutte contre la désinformation. Les *task forces* Sud et Balkans occidentaux visaient initialement à renforcer la communication stratégique de l'Union européenne dans ces régions. Ces deux dernières structures ont vu leurs objectifs élargis à la suite des conclusions du Conseil de décembre 2019 invitant la haute représentante de l'UE pour les

¹ [Audition](#) du 29 mai 2024.

affaires étrangères et la politique de sécurité Federica Mogherini à renforcer la lutte contre la désinformation.

L'action de riposte face aux opérations d'influence menée par le SEAE se concentre essentiellement sur la Russie. En termes de ressources humaines, la *task force* dédiée au voisinage oriental concentre une majorité des effectifs affectés à la lutte contre la désinformation. Les deux autres groupes de travail sont ainsi dotés de moins de cinq agents chacun. En outre, **la plateforme *EUvsDisinfo*, créée en 2015 qui constitue le volet le plus visible de l'action du SEAE en la matière, relaie essentiellement des contenus relatifs à la Russie.** Ce site, alimenté par la *East StratCom Task Force*, produit des contenus dans cinq langues européennes. **La qualité et la pertinence de ses productions ont cependant été négativement évaluées** par la Cour des comptes européenne dans un rapport de 2021¹. De plus, ses productions sont quasi exclusivement consacrées à la Russie et peu aux autres menaces informationnelles. À titre d'exemple, la page « Chine » de cette plateforme ne comporte que cinq articles, contre 137 pour la désinformation russe à l'égard de l'Ukraine.

De manière générale, les moyens du SEAE dans la lutte contre les manœuvres informationnelles **paraissent insuffisants compte tenu de l'ampleur de la menace**. Lors du déplacement de la Commission d'enquête, Mme Aude Maio-Coliche, directrice Communication stratégique et prospective au SEAE, a confirmé que **seule une quinzaine de personnes travaillaient à temps plein sur les FIMI au sein de cette administration**. Le SEAE s'efforce de compléter son action à Bruxelles par le déploiement de *StratCom officers* dans les délégations de l'Union dans les pays tiers.

La commission d'enquête a également noté, lors de son déplacement à Bruxelles, une coordination perfectible entre les services du SEAE et ceux de la direction générale de la communication (DG COMM), cette dernière participant pourtant à la lutte contre la désinformation.

c) La montée en puissance de la communication stratégique de l'Otan

Depuis 2014 et la montée de la menace hybride russe en Europe, l'Otan a également renforcé ses moyens de lutte contre les opérations d'influence. Cette démarche découle d'un mandat clair fixé par les États parties au traité de Washington. Dans un communiqué publié à l'issue du sommet de Vilnius le 11 juillet 2023, les chefs d'État et de gouvernement des pays membres ont indiqué « *que les opérations hybrides menées contre des Alliés pourraient atteindre le seuil correspondant à une attaque armée et conduire le Conseil à invoquer l'article 5 du traité de Washington* ». Les menaces hybrides peuvent ainsi déclencher le principe de sécurité collective garanti par le traité fondateur de l'organisation.

¹ Cour des comptes européenne, [La Désinformation concernant l'UE : un phénomène sous surveillance, mais pas sous contrôle](#), rapport spécial n° 09/2021, juin 2021.

Plus spécifiquement, la déclaration de Vilnius confirme la volonté de « faire face à la désinformation et à la mésinformation, notamment au moyen d'une communication stratégique positive et efficace ». À cet égard, l'Alliance atlantique dispose de capacités opérationnelles pour identifier et dénoncer les attaques informationnelles. Ces capacités reposent sur la « **division diplomatie publique** » (PDD), placée au sein du Secrétariat international. Elle interagit avec les autorités militaires de l'Otan, le Commandement allié opérations (ACO) et le Commandement allié transformation (ACT), chargées de la communication sur les opérations.

L'approche de lutte contre la désinformation repose sur une approche en deux temps : **une analyse de l'environnement informationnelle, suivie d'une communication avec le grand public**. Cette communication vise notamment à contrer les récits de désinformation. La PDD a ainsi créée une page dédiée « *Mise au point* » sur laquelle **elle réfute les principaux « mythes » répandus par la Russie sur l'Otan**. Pour autant, la division diplomatie publique n'opère pas elle-même d'actions d'attribution d'opérations d'influence informationnelle visant des États membres, prérogative qui relève selon elle de la souveraineté nationale.

Exemple d'une réfutation de « mythe » relayé par la Russie sur l'Otan



Le mythe :

L'OTAN est en guerre avec la Russie en Ukraine



Les faits :

L'OTAN n'est pas en guerre contre la Russie. Nous ne cherchons pas la confrontation avec la Russie. L'Alliance apporte son soutien à l'Ukraine, qui exerce son droit à la légitime défense, consacré par la [Charte des Nations Unies](#). Face aux actions agressives de la Russie, nous continuons de renforcer notre posture de dissuasion et de défense pour ne laisser aucun doute sur le fait que l'OTAN est prête à protéger et à défendre chaque Allié.

L'Alliance a une vocation défensive. Notre tâche principale est de préserver la sécurité de nos pays. Au [sommet de Vilnius](#), les Alliés ont réaffirmé leur attachement sans faille à défendre chaque centimètre carré du territoire de l'Alliance, et ce en permanence, ainsi qu'à protéger la population de leurs pays, soit un milliard de personnes, et à y préserver la liberté et la démocratie, conformément à [l'article 5](#) du traité de Washington.

Source : Site internet de l'Otan

L'Alliance travaille étroitement avec deux centres d'excellence en lien avec les opérations d'influence. Il s'agit d'une part du centre européen pour la lutte contre les menaces hybrides (*Hybrid CoE*), créé en 2017 et basé à Helsinki en Finlande. Ce centre, dont le fonctionnement se rapproche d'un *think tank* et qui regroupe des États membres de l'Otan et de l'UE, vise à améliorer la compréhension des menaces hybrides pour proposer des contre-

mesures d'ensemble. D'autre part, un centre d'excellence pour la communication stratégique, directement rattaché à l'Otan situé à Riga, permet aux États membres de l'Otan de renforcer leurs capacités de communication stratégique. Une troisième structure, le centre d'excellence pour la cyberdéfense en coopération, situé à Tallinn en Estonie, participe à cet écosystème.

Selon la secrétaire générale adjointe de l'Otan pour la diplomatie publique, Marie-Doha Besancenot, interrogée par la délégation de la commission d'enquête lors de son déplacement à Bruxelles, **l'organisation cherche à renforcer ses capacités de lutte contre les opérations d'influence informationnelles pour :**

- renforcer son corpus doctrinal en la matière, notamment en adoptant le concept de *FIMI*, développé par l'Union européenne ;
- acquérir des capacités de mise en commun de l'expérience des États membres, en recensant les opérations dont ces derniers ont été les victimes.

2. La mise en œuvre du régime des mesures restrictives de l'Union européenne comme entrave aux opérations d'influence

En complément de ses actions de communication stratégique, la diplomatie coercitive de l'Union européenne peut intervenir pour entraver les opérations d'influence malveillante.

L'Union européenne dispose en effet, dans le cadre de la politique étrangère et de sécurité commune (PESC), d'un régime de mesures restrictives. Ces dernières peuvent intervenir en complément de sanctions diplomatiques, comme le rappel d'un représentant de l'Union auprès d'un État tiers.

Les mesures restrictives, dont le régime est fixé par l'article 215 du traité sur le fonctionnement de l'Union européenne (TFUE) peuvent comprendre des sanctions sectorielles dirigées contre des États (restrictions aux importations et exportations, restrictions à la fourniture de services...) et des mesures ciblées « *à l'encontre de personnes physiques ou morales, de groupes ou d'entités non étatiques* » (gel des avoirs, interdiction de pénétrer sur le territoire de l'Union...). Ces sanctions sont dites « autonomes » lorsqu'elles n'interviennent pas en exécution à une résolution obligatoire du Conseil de sécurité de l'ONU.

L'adoption de mesures restrictives suit une procédure à « *double détente* ». D'une part, une décision PESC adoptée par le Conseil à l'unanimité et prévoyant des sanctions. D'autre part, un acte portant adoption des « *mesures nécessaires* », généralement un règlement d'application, adopté à la majorité qualifiée par le Conseil sur initiative conjointe du haut représentant et de la Commission. Les États membres, exécutifs de droit commun de l'Union, en assurer l'application au niveau national.

En matière d'opérations d'ingérence à visée d'influence, le régime de mesures restrictives a pu être mobilisé pour entraver les cybermenaces. La décision (PESC) 2019/797 du Conseil du 17 mai 2019 introduit un régime de mesures restrictives pour contrer les cyberattaques constituant une menace extérieure pour l'Union ou ses États membres. Elle vise tant les personnes physiques responsables de ces attaques que celles apportant un soutien à l'opération ou impliquées de toute autre manière.

Plus récemment, en réaction à l'agression russe contre l'Ukraine et dans un contexte de durcissement des attaques informationnelles prorusses à compter de février 2022, l'Union européenne a établi un régime de sanctions visant à la fois des médias et les responsables individuels d'opérations de désinformation. Sur un plan juridique, ces mesures restrictives se sont rattachées au régime général des sanctions relatives au conflit en Ukraine défini par la décision 2014/145/PESC concernant des mesures restrictives eu égard aux actions compromettant ou menaçant l'intégrité territoriale, la souveraineté et l'indépendance de l'Ukraine.

En premier lieu, au lendemain de l'invasion russe, l'UE a rapidement adopté des sanctions visant à interdire la diffusion de plusieurs médias russes. Ce point sera plus particulièrement développé *infra*.

En second lieu, des mesures ciblées visant les personnes responsables de la conduite d'opérations de désinformation ont été mises en place. Ces mesures restrictives ciblées concernent à la fois les personnes et les entités responsables de l'opération. À titre d'exemples :

- la décision (PESC) 2023/1566 du Conseil du 28 juillet 2023¹ a prévu des mesures restrictives à l'encontre de sept personnes² et cinq entités russes responsables de la conduite d'une campagne numérique de manipulation de l'information *RRN/Doppelgänger*. Parmi ces entités, Social Design Agency et Structura National Technologies sont des entreprises russes d'informatique impliquées dans la duplication de sites d'institutions et de médias dans le cadre de la campagne RRN. L'agence de presse Inforos, faux-nez du renseignement militaire russe est aussi sanctionnée, de même que l'Institut de la diaspora russe, une de ses extensions. Enfin, ANO Dialog, ONG produisant et diffusant de fausses informations sur la guerre en Ukraine est ciblée par la décision ;

- la décision (PESC) 2024/1508 du Conseil du 27 mai 2024³, a institué des mesures restrictives à l'encontre de « *Voice of Europe* », média financé par

¹ [Décision \(PESC\) 2023/1566 du Conseil du 28 juillet 2023](#) modifiant la décision 2014/145/PESC concernant des mesures restrictives eu égard aux actions compromettant ou menaçant l'intégrité territoriale, la souveraineté et l'indépendance de l'Ukraine.

² Timofey Vassiliev, Ilya Gambachidze, Aleksandr Starunsky, Anastasia Kirillova, Nina Dorokhova, Sergey Panteleyev et Denis Tyurin.

³ [Décision \(PESC\) 2024/1508 du Conseil du 27 mai 2024](#) modifiant la décision 2014/145/PESC concernant des mesures restrictives eu égard aux actions compromettant ou menaçant l'intégrité territoriale, la souveraineté et l'indépendance de l'Ukraine.

la Russie pour diffuser des contenus de désinformation, et de deux anciens politiques et hommes d'affaires ukrainiens liés à ce média, Artem Marchevskyi et Viktor Medvedchuk. Ces deux personnes auraient financé, au travers de *Voice of Europe*, des opérations d'influence visant des personnes politiques en Europe et de désinformation.

III. RÉGULATION ET RÉSILIENCE : UNE IMPLICATION INÉGALE DES DIFFÉRENTS ACTEURS DES POLITIQUES PUBLIQUES

Nos politiques publiques concourant à la lutte contre les influences étrangères malveillantes ne se limitent pas aux actions, par essence régaliennes de détection et de réponse, détaillées dans les sections précédentes.

S'agissant d'un phénomène qui concerne la société dans son ensemble, la commission d'enquête s'est attachée à passer en revue les principales politiques publiques mobilisables pour concourir à la résilience de la société face à ces opérations, sans pouvoir prétendre à l'exhaustivité.

A. LA RÉGULATION DE L'ESPACE MÉDIATIQUE ET DES PLATEFORMES : DES PROGRÈS IMPORTANTS RÉALISÉS AU COURS DES DERNIÈRES ANNÉES

1. Le contrôle des médias étrangers : un renforcement important au cours des dernières années

La façon la plus évidente de lutter contre les influences étrangères malveillantes dans la sphère médiatique est d'exercer un **contrôle sur les médias étrangers**. En France, ce contrôle relève de l'**Autorité de régulation de la communication audiovisuelle et numérique (Arcom)**.

a) Un cadre juridique complexe, qui confère à l'Arcom d'importantes prérogatives

Le droit français permet d'opérer une distinction entre les médias français et les médias étrangers.

En premier lieu, celui-ci tend à protéger les premiers d'influences étrangères possible en régulant la structure de leur capital. Aussi, l'article 40 de la loi du 30 septembre 1986 relative à la liberté de communication prévoit que, sous réserve des engagements internationaux de la France, l'autorisation relative à un service de radio ou de télévision par voie hertzienne terrestre assuré en langue française ne peut être accordée à une société dans laquelle plus de 20 % du capital social ou des droits de vote sont détenus, directement ou indirectement, par des personnes de nationalité étrangère. Sous la même réserve, il prévoit qu'aucune personne de nationalité étrangère ne peut

procéder à une acquisition ayant pour effet de porter, directement ou indirectement, la part du capital détenue par des étrangers à plus de 20 % du capital social ou des droits de vote dans les assemblées générales d'une société titulaire d'une telle autorisation.¹

Le droit applicable aux chaînes étrangères (en l'occurrence extra-européennes) est fondé sur le principe de liberté de réception. Toutefois, ces chaînes doivent respecter les règles découlant de la directive sur les services de médias audiovisuels (directive « SMA »)², transposée dans les droits nationaux, et qui prennent en compte, en particulier, les exigences liées à la protection du public et à l'ordre public.

S'agissant de ces médias, le premier enjeu qui se pose est celui de la compétence du régulateur national.

La détermination de l'État membre compétent à l'égard d'une chaîne extra européenne reçue dans l'Union européenne ou sur le territoire d'un État partie à la convention européenne sur la télévision transfrontière (CETT) relève de règles fondées sur la seule diffusion satellitaire. S'agissant plus particulièrement de l'Union européenne, la directive SMA fixe comme critère principal celui de la localisation de la liaison montante entre le lieu d'émission du service et le satellite chargé d'en assurer la diffusion, et comme critère secondaire celui de la nationalité de la capacité satellitaire.

Ainsi, en application de ces critères, repris à l'article 43-4 de la loi du 30 septembre 1986 précitée, si la liaison montante est localisée sur le territoire d'un État membre de l'Union européenne, c'est cet État membre qui est compétent à l'égard du service. Si la liaison montante est située en dehors du territoire de l'Union européenne, c'est l'État membre dans lequel est établi l'opérateur de capacités satellitaires qui est compétent. **Lors de son audition devant la commission d'enquête, le président de l'Arcom a souligné la grande complexité et la difficulté d'application de ces dispositions³.**

En tout état de cause, il résulte de ces règles, compte tenu de l'activité de l'opérateur satellitaire Eutelsat, et, dans une moindre mesure, de l'activité de liaisons montantes en France de l'opérateur Globecast (Orange), la France est compétente sur plusieurs centaines de services de télévision extra européens, en particulier de chaînes d'Afrique du Nord et du Moyen-Orient diffusées par des satellites d'Eutelsat centrés sur cette région mais pouvant être reçues dans le sud de l'Europe, ou, par exemple, de chaînes russes reçues sur le territoire ukrainien, État partie à la CETT.

¹ Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

² Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels.

³ [Audition](#) du 19 mars 2024.

Si ces services sous compétence française sont dispensés de conventionnement avec l'Arcom, ils sont cependant **soumis aux obligations de la loi du 30 septembre 1986 même loi et au contrôle du régulateur**¹.

Pour mémoire, l'Arcom dégage de cette loi (en particulier ses articles 1^{er} et 3) et des normes supérieures sept principaux thèmes de déontologiques : le respect de la dignité de la personne humaine, la sauvegarde de l'ordre public, la lutte contre les discriminations, l'honnêteté et l'indépendance de l'information, le traitement des affaires judiciaires et le respect du droit à la vie privée². Comme le relève cependant la commission d'enquête, le rattachement d'un contenu à une opération d'ingérence étrangère ne figure à ce stade pas explicitement parmi ces thèmes, bien que celle-ci puisse être appréhendée indirectement au travers de la sauvegarde de l'ordre public ou encore l'honnêteté et l'indépendance de l'information.

En cas de méconnaissance d'une de ces obligations, l'Arcom peut mettre en œuvre les prérogatives prévues par la loi du 30 septembre 1986, soit :

- mettre en œuvre une procédure de sanction à l'égard du service (article 42) ;
- mettre en demeure Eutelsat de faire cesser la diffusion de ce service (article 42-1) ;
- demander au président de la section du contentieux Conseil d'État qu'il ordonne en référé à Eutelsat de le faire (article 42-10).

La prérogative de mise en demeure prévue à l'article 42-1 de la loi précitée a récemment été mise en application à l'encontre de deux chaînes russes au titre de manquements pouvant être considérés comme participant d'une politique d'influence étrangère :

- la mise en demeure d'Eutelsat par l'Arcom, par une décision n° 2022-491 du 27 juillet 2022, de cesser la diffusion du service « NTV Mir » ;
- la mise en demeure d'Eutelsat par l'Arcom, par une décision n° 2022-763 du 14 décembre 2022, de cesser la diffusion des services « Rossiya 1 », « Perviy Kanal » et « NTV ».

Dans le cadre du dispositif de contrôle des médias étrangers, les services de médias audiovisuels à la demande (SMAD), diffusés sur Internet uniquement, ont longtemps constitué un « angle mort ».

L'article 14 de la loi du 21 mai 2024 visant à sécuriser et réguler l'espace numérique (SREN)³ est très récemment venue combler cette lacune, afin de prévoir que les prérogatives conférées par l'Arcom par la loi

¹ Conformément aux dispositions du III de l'article 33-1 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

² Pour plus de détails, voir la [page dédiée](#) sur le site internet de l'Arcom.

³ Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

du 30 septembre 1986 soient bien applicables à ces services dès lors qu'ils sont diffusés en France et ne relèvent pas de la compétence d'un autre État membre de l'Union européenne, d'un autre État partie à l'accord sur l'Espace économique européen ou d'un autre État partie à la convention européenne sur la télévision transfrontière du 5 mai 1989 (CETT).

b) La nécessité d'une articulation avec la politique étrangère de l'Union européenne est mise en évidence par l'offensive informationnelle liée au conflit en Ukraine

L'offensive menée par la Russie dans les espaces informationnels occidentaux dans le cadre du conflit en Ukraine a impliqué l'adoption d'une mesure forte par l'Union européenne, avec l'interdiction de diffusion des médias d'État russes menant des actions de propagande, soit en l'espèce *Russia Today* et *Sputnik*, bien que la portée effective de ces sanctions doive être nuancée compte tenu des manœuvres de contournement opérées par ces chaînes (voir *Première partie, IV*).

Au plan juridique, cette mesure a revêtu la forme d'un règlement de l'Union européenne pris non pas au titre d'une compétence de régulation des médias mais de la politique étrangère et de sécurité commune (PESC)¹.

S'est ainsi posée la question de l'articulation des compétences entre l'Union et le régulateur national au titre de l'application de ces sanctions, qui a également trouvé une réponse avec l'article 14 de la loi SREN précité, prévoyant expressément que l'Arcom peut mettre en demeure puis sanctionner les opérateurs soumis à la loi du 30 septembre 1986 (éditeurs, distributeurs, opérateurs satellitaires...) qui ne font pas cesser la diffusion de médias sous sanction européenne et, d'autre part, que l'Arcom peut saisir en référé le président de la section du contentieux à cette même fin.

Le récent règlement européen relatif à la liberté des médias (dit règlement « EMFA »), qui entrera en vigueur en 2025, entend également améliorer la gestion commune des problématiques liées à la propagande déployée par les médias étrangers, citant expressément dans ses considérants la problématique des « *campagnes internationales systématiques de manipulation de l'information et d'ingérence menées depuis l'étranger en vue de déstabiliser l'Union dans son ensemble ou certains de ses États membres* ». Son article 17 crée à cette fin un cadre de coordination de l'action des régulateurs nationaux *via* le futur Comité européen pour les services de médias, qui permet un partage accru d'information et favorise le développement d'une approche commune par les États membres².

¹ Règlement (UE) 2022/350 du Conseil du 1^{er} mars 2022 modifiant le règlement (UE) n° 833/2014 concernant des mesures restrictives en égard aux actions de la Russie déstabilisant la situation en Ukraine.

² Règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE (règlement européen sur la liberté des médias).

c) *La lutte contre les manipulations de l'information par les médias étrangers*

Par ailleurs, la **loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information**¹ a introduit dans la loi du 30 septembre 1986 des dispositions visant à lutter contre la participation à des actes de manipulation de l'information de services établis en France et donc conventionnés par l'Arcom, mais qui sont contrôlés ou placés sous l'influence d'un État étranger. À ce titre, l'Arcom peut en particulier :

- ordonner, pendant les trois mois qui précèdent un scrutin national et durant ce scrutin, la suspension de la diffusion d'un tel service s'il diffuse, de façon délibérée, de fausses informations de nature à altérer la sincérité du scrutin (article 33-1-1 de la loi du 30 septembre 1986) ;

- résilier unilatéralement la convention d'un tel service, après mise en demeure, lorsqu'il porte atteinte aux intérêts fondamentaux de la Nation, dont le fonctionnement régulier de ses institutions, notamment par la diffusion de fausses informations (article 42-6 de la même loi).

D'après les informations transmises par l'Arcom à la commission d'enquête, ces dispositifs n'ont cependant pas trouvé lieu à s'appliquer à ce jour.

Les travaux de la commission d'enquête ont cependant permis de mettre en évidence les moyens limités de l'Arcom pour accomplir pleinement son rôle de régulateur vis-à-vis des médias étrangers relevant de sa compétence, en particulier en termes de compétences linguistiques internes. D'après ses réponses au questionnaire du rapporteur, l'Arcom ne dispose que d'un agent arabisant. En revanche, elle doit faire appel à un traducteur extérieur pour les besoins d'analyse de programmes dans d'autres langues étrangères (mandarin, russe...).

2. La lutte contre les manipulations de l'informations sur les plateformes en ligne : des moyens juridiques renforcés, dans le cadre d'une approche encore trop timorée

Les médias étrangers constituent certes un vecteur important des opérations d'influence malveillante conduits par nos compétiteurs étrangers, mais pas le principal. Comme l'a largement montré le présent rapport, ces opérations se déploient de façon massive sur les plateformes numériques, en exploitant leur modèle économique, notamment en recourant à des *trolls* ou en produisant des contenus humoristiques répondant aux caractéristiques de la culture des usagers des plateformes (mèmes).

Comme le résume l'Ambassadeur pour le numérique, Henri Verdier, lors de son audition par la commission d'enquête : « *les réseaux sociaux sont extraordinairement vulnérables aux opérations de désinformation, et ce pour*

¹ Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

plusieurs raisons. Tout d'abord, leur modèle économique repose sur *l'économie de l'attention*. Or pour capter l'attention, le sensationnalisme, le conspirationnisme, les propos excessifs et la colère sont efficaces. C'est humain de notre côté ; c'est mécanique du leur, avec des algorithmes qui présentent plus souvent aux utilisateurs ce qu'ils regardent le plus, créant ainsi des montées aux extrêmes. Ensuite, des mécanismes sont liés au design même de ces solutions, avec des bulles de filtres, qui enferment les utilisateurs dans un *entre-soi* où ils ne voient plus que des gens qui pensent comme eux »¹.

La difficulté posée par les contenus de désinformation sur les plateformes et mis au service d'opérations d'ingérence étrangères résulte du fait que ceux-ci ne sont pas nécessairement en soi illégaux, et peuvent très bien relever du champ de la liberté d'expression. Face à des contenus violant la loi (contenus racistes ou incitant à la haine, faisant l'apologie du terrorisme, etc.) les autorités, notamment alertées par la voie d'un signalement sur la plateforme Pharos ou directement par la plateforme, peuvent demander à celle-ci le retrait des contenus concernés et engager des poursuites pénales contre les auteurs.

Si des dispositifs contraignants ont été pris pour contrôler certaines opérations de désinformation, en particulier dans un contexte électoral ou dans le cadre d'un régime de sanctions européennes, le régime de régulation des plateformes à l'échelle européenne, qui a fait d'importants progrès au cours des années récentes, reste trop timoré.

a) *L'existence du dispositifs contraignants dans des contextes bien déterminés*

(1) Les manipulations de l'information en contexte électoral

La loi précitée du 22 décembre 2018 relative à la lutte contre la manipulation de l'information a mis en place plusieurs outils pour lutter contre les campagnes de désinformation massives dans les contexte électoraux, propices aux opérations d'ingérence informationnelle.

Outre la possibilité, mentionnée *supra*, de faire cesser la diffusion de tels contenus par un média étranger, cette loi permet également d'agir en direction des principales plateformes.

Ainsi, l'article L. 163-1 du code électoral prévoit certaines obligations applicables aux opérateurs de ces plateformes pendant les trois mois précédant le premier jour du mois d'élections générales et jusqu'à la date du tour de scrutin où celles-ci sont acquises :

- fournir à l'utilisateur une information loyale, claire et transparente sur l'identité de la personne physique ou sur la raison sociale, le siège social et l'objet social de la personne morale et de celle pour le compte de laquelle, le cas échéant, elle a déclaré agir, qui verse à la plateforme des rémunérations

¹ [Audition](#) du 28 mars 2024.

en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général ;

- fournir à l'utilisateur une information loyale, claire et transparente sur l'utilisation de ses données personnelles dans le cadre de la promotion d'un contenu d'information se rattachant à un débat d'intérêt général ;

- rendre public le montant des rémunérations reçues en contrepartie de la promotion de tels contenus d'information lorsque leur montant est supérieur à un seuil déterminé.

L'article L. 163-2 du même code prévoit quant à lui un dispositif permettant à l'autorité judiciaire, au cours de la même période, de demander à ce que les plateformes fassent cesser la diffusion de contenus de désinformations diffusées de façon massive et artificielle. Sont ainsi visées les « *allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir sont diffusées de manière délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne* ».

Il est prévu que le juge des référés peut être saisi à cette fin par le ministère public, de tout candidat, de tout parti ou groupement politique ou de toute personne ayant intérêt à agir. Le juge des référés se prononce dans un délai de 48 heures à compter de la saisine. En cas d'appel, la cour se prononce dans un délai de 48 heures à compter de la saisine.

Ce dispositif marque une rupture importante puisqu'il s'agit d'un cas unique permettant au juge de demander la cessation de la diffusion de fausses informations par les plateformes quand bien même ces contenus ne sont pas illégaux. Il est à noter que le dispositif ne cible pas spécifiquement des contenus d'origine étrangère. La référence à une diffusion « *artificielle ou automatisée et massive* » fait écho à la notion d'ingérence numérique étrangère (voir *Première partie, IV*).

De nouvelles règles en la matière ont notamment été adoptées au niveau de l'Union européenne avec le récent règlement sur la publicité politique¹, qui trouve notamment à s'appliquer sur les plateformes.

Ce texte pose comme une nouvelle exigence de droit commun, applicable aux acteurs européens comme extra-européens, que la publicité politique soit clairement étiquetée, permettant aux citoyens de voir pourquoi ils ont été ciblés, qui a sponsorisé la publicité, les montants engagés et les scrutins concernés. En outre, les nouvelles règles n'autorisent le ciblage des utilisateurs que si ces derniers ont consenti à la collecte de leurs données personnelles.

Pour lutter contre la désinformation et les ingérences de commanditaires non européens, est notamment prévue **l'interdiction pour les**

¹ Règlement (UE) 2024/900 du Parlement européen et du Conseil du 13 mars 2024 relatif à la transparence et au ciblage de la publicité à caractère politique.

entités de pays tiers de parrainer la publicité politique dans l'Union européenne au cours des trois mois précédant une élection qu'elle soit locale, nationale ou européenne, ainsi que les référendums.

Si cette législation constitue une avancée très positive, la commission d'enquête relève que sa correcte application pourrait s'avérer complexe dans la pratique et donc peu efficace en l'état.

(2) Le cas des contenus relayés par des médias sous sanction européenne

En matière de mesures contraignantes à l'égard des plateformes, il convient également de souligner qu'une nouvelle étape a été franchie avec l'article 14 de la loi SREN précitée avec la possibilité pour l'Arcom de demander d'utiliser ses pouvoirs, de mise en demeure, de demande de blocage, de déréférencement et de sanction à l'égard d'un opérateur de plateforme afin de faire cesser la diffusion ou la mise à disposition des contenus dont la diffusion est interdite en application des dispositions des sanctions prises par le Conseil de l'Union européenne.

b) La régulation aux niveaux national et européen : des progrès importants, mais une approche qui reste encore timorée

(1) Dès 2018, la France a mis en place un cadre juridique instituant une obligation de moyens pour les plateformes en matière de lutte contre la désinformation

En adoptant la loi précitée du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, la France a instauré un cadre précurseur **fondé sur des obligations de moyens et de transparence** qui **incombent aux opérateurs de plateforme en ligne en France**.

Cette loi impose aux plateformes de mettre en place de toute une série de mesures en vue de lutter contre la diffusion de fausses informations susceptibles de troubler l'ordre public ou d'altérer la sincérité d'un scrutin, sans cibler expressément l'origine étrangère de ces contenus.

Dans le détail, son article 11 prévoit notamment que celles-ci mettent en place un dispositif facilement accessible et visible permettant à leurs utilisateurs de signaler de telles informations, notamment lorsque celles-ci sont issues de contenus promus pour le compte d'un tiers.

Il prévoit également que celles-ci mettent en œuvre des mesures complémentaires pouvant notamment porter sur :

1° la transparence de leurs algorithmes ;

2° la promotion des contenus issus d'entreprises et d'agences de presse et de services de communication audiovisuelle ;

3° la lutte contre les comptes propagant massivement de fausses informations ;

4° l'information des utilisateurs sur l'identité de la personne physique ou la raison sociale, le siège social et l'objet social des personnes morales leur versant des rémunérations en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général ;

5° l'information des utilisateurs sur la nature, l'origine et les modalités de diffusion des contenus ;

6° l'éducation aux médias et à l'information.

Il est prévu que ces mesures, ainsi que les moyens qu'ils y consacrent, sont rendus publics, et que l'Arcom en dresse un bilan périodique, le dernier en date ayant été publié en décembre 2022 au titre de l'année 2021¹.

(2) Une approche reprise par le Règlement sur les services numériques, dit « DSA »

Cette approche a été **reprise par le Règlement européen sur les services numériques (RSN)**, communément appelé « DSA » (pour *Digital Service Act*)², qui a conduit à une adaptation du cadre français *via* la loi SREN précitée.

Dans le cadre de ce règlement, les très grandes plateformes et très grands moteurs de recherche (dit « VLOPSEs ») désignés par la Commission en avril 2023 sont **soumis à des exigences renforcées d'identification et d'évaluation des risques systémiques** liés à la diffusion de contenus affectant « *le discours civique, les processus électoraux et la sécurité publique* », ce qui inclut plus particulièrement les contenus de désinformation, y compris ceux qui, sans être illégaux, seraient préjudiciables. En revanche, le DSA et la loi SREN ne confient ni à l'Arcom, ni à la Commission compétence pour intervenir sur un contenu individuel donné.

La loi SREN désigne l'Arcom comme autorité en charge de superviser la mise en œuvre du règlement en France, aux côtés des autres autorités compétentes que sont la Commission nationale de l'informatique et des libertés (CNIL) et la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), et lui confie plus généralement le soin, en la désignant coordinateur pour les services numériques (CSN), de veiller à l'application cohérente du règlement en France, ce qui apparaît essentiel dans un contexte où la réussite du DSA supposera une coordination efficace des autorités compétentes.

En lien avec le Comité des coordinateurs pour les services numériques, l'Arcom est désormais en mesure d'exercer ses compétences,

¹ Arcom, *Lutte contre la manipulation de l'information sur les plateformes en ligne. Bilan annuel des moyens et des mesures mises en œuvre par les plateformes en ligne en 2021*

² Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques)

notamment en signalant une infraction supposée, étant entendue que celle-ci ne peut porter que sur les moyens mis en œuvre par les plateformes et non sur les contenus eux-mêmes, ou en demandant le déclenchement du protocole de crise, et de proposer son expertise en matière d'analyse des risques systémiques à la Commission, qui détient une compétence exclusive en la matière sur les VLOPSEs.

La loi SREN maintient également ainsi le pouvoir de recommandation de l'Arcom à l'attention des VLOPSEs en matière de lutte contre la désinformation, tout en continuant de lui confier la mission de publier un **bilan périodique**. **Il est toutefois à noter qu'alors que ce bilan a jusqu'ici été présenté par l'Arcom comme annuel, celui relatif à l'année 2022 n'a toujours pas été publié.**

Par ailleurs, l'Arcom participe à l'évaluation des engagements des mesures du Code européen renforcé de bonnes pratiques contre la désinformation du 16 juin 2022¹, révisé et adopté avant le DSA, qui sont susceptibles de constituer des mesures d'atténuation des risques systémiques. L'Autorité a indiqué à la commission d'enquête avoir pu analyser les rapports de septembre 2023 des VLOPSEs signataires du Code (comme Instagram, Facebook, LinkedIn, Bing, Google Search, YouTube et TikTok), en partenariat avec d'autres régulateurs européens.

Au titre spécifique de la manipulation de l'information liée à des opérations d'ingérence numérique étrangères, l'Arcom et Viginum ont signé fin 2023 une convention pour travailler à un renforcement de leur collaboration permettant des échanges respectifs d'informations, notamment en vue de la mise en œuvre du DSA et dans la perspective des événements majeurs de 2024 (élections européennes, jeux Olympiques et Paralympiques). Cette convention a pour principal objectif de faire en sorte que les travaux de détection conduits par Viginum puissent nourrir l'analyse des techniques, tactiques et procédures de manipulation de l'information dans le cadre de l'application du DSA.

Il est enfin à noter que, dans la perspective des élections européennes de juin 2024, l'Arcom a publié le 7 mars 2024 des préconisations qui permettent de relayer les mesures prévues dans le projet de lignes directrices sur les risques spécifiques aux processus électoraux soumis par la Commission européenne à consultation publique en février 2024, en appelant les opérateurs à tirer toutes les conséquences des règles relatives à l'organisation du scrutin prévues spécialement en France, comme la période de silence électoral².

¹ Commission européenne, *Code européen renforcé de bonnes pratiques contre la désinformation du 16 juin 2022* (disponible en [version anglaise](#)).

² Arcom, [Préconisations relatives à la lutte contre la manipulation de l'information sur les plateformes en ligne en vue des élections au Parlement européen du 6 au 9 juin 2024](#).

(3) Les enjeux liés à la mise en œuvre du DSA ont conduit l'Arcom à renforcer sa coopération avec Viginum

Le cadre réglementaire applicable à Viginum prévoit expressément que ce service est tenu de fournir toute information utile à l'Arcom dans l'accomplissement des missions qui lui sont confiées par la loi du 30 septembre 1986 précitée¹.

L'exercice de mission a déjà donné lieu à la transmission de plusieurs notes par Viginum, au titre d'opérations d'ingérences numériques étrangères qu'elle a détectées dans le contexte de périodes sensibles (voir tableau ci-dessous).

Il est à noter qu'une note de Viginum relative à des manquements à la modération de la plateforme X (ex-Twitter) a donné lieu à une transmission à la Commission européennes.

Notes transmises par Viginum à l'Arcom

Catégories	Notes transmises
Notes relatives aux élections présidentielles et législatives	- 18 notes de détection élections présidentielles - notes de caractérisation élections présidentielles - 7 notes de détection élections législatives - 1 note de caractérisation élections législatives
Notes relatives à certains événements/crises	1 note relative au conflit Israël/Hamas
Notes relatives aux risques systémiques engendrés par les plateformes	1 note relative aux manquements à la modération de la plateforme X (transmise à la Commission européenne)

Source : commission d'enquête, d'après les réponses de Viginum au questionnaire du rapporteur.

Les missions confiées à l'Arcom au titre de la mise en œuvre du DSA ont également conduit à un rapprochement avec Viginum, qui a donné lieu à la signature d'une convention cadre de partenariat signée le 4 juillet 2024².

¹ Article 3 du décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères ».

² [Convention cadre de partenariat](#) entre l'Arcom et Viginum, 4 juillet 2024.

- (4) La Commission européenne a déjà fait un usage effectif des pouvoirs qui lui sont conférés par la DSA

Il est à noter que la Commission européenne, où s'est rendue une délégation de la commission d'enquête dans le cadre d'un déplacement effectué à Bruxelles, a déjà fait un usage effectif de ces pouvoirs pour appliquer le DSA.

Premièrement, elle a ouvert **plusieurs procédures formelles** à l'égard des différentes plateformes, soit une procédure qui habilite la Commission à prendre de nouvelles mesures d'exécution, telles que des mesures provisoires, et des décisions de non-conformité, si nécessaire.

En décembre 2023, la Commission a d'abord ouvert une procédure formelle afin d'évaluer si X pourrait avoir enfreint la législation sur les services numériques dans des domaines liés à la gestion des risques, à la modération des contenus, aux interface truquée (« *dark patterns* »), à la transparence de la publicité et à l'accès aux données pour les chercheurs. Le 12 juillet 2024, elle a **informé X de son avis préliminaire selon lequel la plateforme enfreint les règles du DSA**.

En avril 2024, elle a ouvert une procédure formelle afin d'évaluer les infractions présumées aux politiques et pratiques de Meta en matière de publicité trompeuse et de contenu politique sur ses services.

En outre, la Commission a ouvert deux procédures formelles à l'encontre de TikTok, en se concentrant particulièrement sur la protection des mineurs.

Enfin, **en ce qui concerne spécifiquement l'utilisation des techniques d'intelligence artificielle (IA)** pour diffuser des hypertrucages (*deep fakes*), la Commission a officiellement envoyé, en mars, des demandes de renseignements horizontales au titre de la législation sur les services numériques à deux très grands moteurs de recherche en ligne et à six très grandes plateformes en ligne, leur demandant de fournir des informations détaillées sur leurs mesures respectives visant à atténuer les risques associés à l'IA générative, telles que les « *hallucinations* », dans lesquelles l'IA fournit de fausses informations, la propagation virale des trucages bruyants, ainsi que la manipulation automatisée de services susceptibles d'induire les électeurs en erreur.

c) Une approche qui reste timorée et lacunaire

- (1) Des plateformes qui restent de simples hébergeurs, sans responsabilité à l'égard des contenus qu'elles diffusent

Si le DSA doit permettre d'accomplir de grands progrès dans la régulation des plateformes en France et à l'échelle européenne, la philosophie du dispositif, fondée sur la seule obligation de moyens, reste insatisfaisante.

En effet, le rapporteur considère que, compte tenu du mode de fonctionnement des plateformes, leur statut de simple « hébergeur », sans responsabilité sur les contenus diffusés par leur intermédiaire, ne permet pas de caractériser adéquatement leur activité.

Comme l'explique en effet Thomas Huchon journaliste spécialiste de ces questions auditionné par la commission d'enquête : « *Il faut arrêter de considérer que ces plateformes sont des tuyaux et plutôt les faire rentrer dans la loi de 1881 sur la liberté de la presse. Pour savoir si ces plateformes doivent entrer dans la loi de 1881, il faut répondre à trois questions. La première est de savoir si ces plateformes diffusent de l'information, ce qui est le cas. La deuxième question est de savoir si elles hiérarchisent et éditorialisent ces informations, ce qui est également le cas, car l'information que voit une personne n'est pas nécessairement la même que celle que voit une autre personne naviguant sur la même plateforme. La troisième question est de savoir si elles gagnent de l'argent en réalisant ces deux premières opérations, ce qui est le cas. Il semble difficile de considérer qu'une plateforme qui diffuse de l'information, hiérarchise et éditorialise de l'information et gagne de l'argent en le faisant ne serait pas un média, mais un simple tuyau. Je pense qu'il existe une forme de contradiction inacceptable, que nous avons acceptée, et que nous sommes aujourd'hui dans un état de fait très désagréable, dans lequel nous sommes un peu pris au piège de nos incompréhensions technologiques depuis quinze ans et de notre passivité sur tous ces sujets* »¹.

David Chavalarias, chercheur, a également pu détailler ce mode de fonctionnement devant la commission d'enquête, et la raison pour laquelle il s'avère particulièrement propice aux ingérences étrangères : « *les plateformes ont mis en place depuis 2018 un fil d'actualité. C'est l'endroit où les personnes consultent la majorité de leurs contenus. Ce que quelqu'un voit sur son fil d'actualité, ce n'est qu'un petit pourcentage de ce que produit son environnement social, moins de 10 %. Il y a donc un filtre entre ce que produisent les personnes auxquelles vous êtes abonné et ce que vous voyez effectivement. Comment ce filtre est-il élaboré ? Nous avons montré qu'entre vos abonnements et ce que vous recevez dans votre fil d'actualité, il y a 50 % de contenus toxiques en plus sur le réseau Twitter, c'est-à-dire des insultes, du dénigrement, des attaques personnelles, etc. Par conséquent cela va déformer la perception des utilisateurs de millions d'utilisateurs. Facebook et Instagram fonctionnent de la même manière et modifient la perception de millions d'utilisateurs vers un environnement plus hostile. Dès que les plateformes optimisent l'engagement, c'est-à-dire dès qu'elles mettent dans les fils d'actualité des utilisateurs les contenus qui ont le plus de clics, de « likes » et de partages, ce qu'elles font depuis 2018, ces biais de négativité apparaissent. C'est un gros problème parce que cela renforce l'hostilité des échanges et, indirectement, les personnalités et les comptes qui s'expriment de manière hostile. La circulation de l'information est modifiée, comme la structure du réseau. Dans le top des 1 % des influenceurs, il y a une surreprésentation de 40 % de personnes qui s'expriment de manière hostile.*

¹ [Audition](#) du 9 avril 2024.

Avec les plateformes comme Facebook, Twitter ou Instagram, qui réunissent plusieurs milliards d'utilisateurs, l'opinion publique se forme dans des environnements où, de manière centralisée, changer une ligne de code permet de changer complètement la manière dont l'information circule mais aussi la manière dont les personnes s'expriment puisque les journalistes et les politiques vont changer leur manière de s'exprimer pour éviter leurs discours ne soient pas diffusés »¹.

Le caractère anonyme des profils inscrits sur les plateformes constitue un facteur de risque supplémentaire. David Chavalarias considère à cet égard que, sans aller jusqu'à lever cet anonymat, il pourrait être envisagé de forcer les plateformes à permettre aux utilisateurs de « *s'authentifier en tant que Français, tout en restant anonyme, sans donner d'autres d'informations, par exemple en passant par un intermédiaire comme France Connect qui certifie que l'utilisateur est français* ». Les utilisateurs pourraient ainsi filtrer les contenus en disant qu'ils ne veulent voir que les contenus émis par leurs compatriotes, ce qui permettrait d'éliminer de nombreuses ingérences propagées à partir de faux comptes »².

Il souligne également l'importance de mieux modérer les publicités ciblées, alors que circuleraient aujourd'hui « des milliers de sur le territoire français, en Italie, en Pologne et en Allemagne ». À cet égard, s'agissant par exemple de Facebook, il estime que la plateforme « *ne modère qu'à peine 20 % des publicités politiques* ».

David Chavalarias a enfin mentionné plusieurs axes de propositions structurantes pour assainir le modèle de fonctionnement des plateformes : défendre les utilisateurs contre les clauses abusives des réseaux sociaux et imposer la portabilité des données et de l'influence sociale

(2) Le cas de TikTok : des recommandations de la commission d'enquête sénatoriale de 2023 qui sont restées lettres mortes

S'agissant en particulier de TikTok, dont le lien à la Chine a été rappelé *supra* (voir *Première partie, III*), la **commission d'enquête du Sénat sur l'utilisation du réseau social TikTok**, son exploitation des données, sa stratégie d'influence³ a ainsi expressément recommandé que cette plateforme soit traitée en éditeur au titre de son fil « Pour toi », qui opère une telle sélection personnalisée de contenus.

Son rapport préconise également **d'imposer des obligations positives à la plateforme, à rebours de la philosophie du DSA, et notamment**

¹ [Audition](#) du 4 juin 2024.

² Dans le compte-rendu de son [audition](#) par la commission d'enquête du 4 juin 2024, David Chavalarias évoque la possibilité de « *forcer les utilisateurs à s'authentifier en tant que Français* ». Dans un courriel en date du 12 juin 2024 adressé au président et au rapporteur de la commission d'enquête, David Chavalarias a précisé que sa proposition consistait à contraindre les plateformes à permettre aux utilisateurs français de s'authentifier en tant que Français, et non à contraindre les utilisateurs eux-mêmes à utiliser cette fonctionnalité.

³ [Rapport n° 831 \(2022-2023\)](#) fait par Claude Malhuret au nom de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence, déposé le 4 juillet 2023.

de modifier son algorithme pour promouvoir des contenus certifiés comme provenant de sources d'information fiables.

Enfin, ce rapport avait recommandé la suspension de TikTok en France et la demande par la France de sa suspension au sein de l'Union européenne pour des raisons de sécurité nationale :

- si TikTok, avant le 1^{er} janvier 2024, n'a pas répondu aux principales questions soulevées par cette commission d'enquête : capital et statuts de la maison-mère ByteDance ; propriété intellectuelle et localisation des ingénieurs qui élaborent l'algorithme ; nature des entités chinoises avec lesquelles TikTok est en relation permanente ; nature des données des utilisateurs transférées en Chine et raison de ces transferts...

- si TikTok, dans le même délai, n'a pas pris les principales mesures demandées par le rapport.

La commission d'enquête ne peut que regretter que ces recommandations soient restées lettres mortes.

(3) Faute d'obligations spécifiques, les plateformes n'ont pas d'obligation de retirer des contenus liés à des opérations d'ingérence étrangères qui ne revêtent pas de caractère illégal

Viginum a indiqué au rapporteur qu'il entretient des relations avec les plateformes reposant sur des échanges ponctuels, visant le plus souvent à solliciter des actions à l'encontre de comptes impliqués dans des manœuvres informationnelles caractérisées. Ces sollicitations peuvent prendre la forme de partages d'éléments techniques, à l'image de ce qui a pu être fait à la suite de la dénonciation publique de la campagne de manipulation de l'information RRN (voir *Première partie, IV*). Viginum peut également être amené à réaliser des actions de sensibilisation des plateformes sur les tentatives de manipulation de leurs services par des acteurs étrangers, comme ce fut le cas aux côtés de l'Arcom et du ministère des affaires étrangères le 2 mai 2024, dans la perspective des élections européennes.

Toutefois, **si les opérateurs de plateforme semblent davantage tenir compte des risques liés à la menace de manipulation de l'information, probablement depuis la mise en œuvre effective du DSA, leur relation avec Viginum demeure encore trop épisodique**. Dans le détail, seule une plateforme a offert un accès API à ses agents : Google/YouTube.

Dans l'hypothèse d'un contenu qui revêtirait un caractère illicite, Viginum a récemment signé une convention avec la plateforme Pharos du ministère de l'Intérieur le 7 décembre 2023, afin d'intégrer Viginum à la liste des « signaleurs de confiance ». Cette qualification permet notamment à Viginum d'obtenir un traitement plus rapide par Pharos.

(4) L'enjeu des manipulations de l'information recourant à l'intelligence artificielle : un problème encore devant nous

Une autre lacune actuelle de la réglementation concerne le recours à l'intelligence artificielle dans le cadre des opérations de manipulation de l'information conduites sur les plateformes, en particulier au moyen d'hypertrucages (*deepfakes*) et d'amplification.

Lors de son audition devant la commission d'enquête, l'Ambassadeur pour le numérique Henri Verdier alertait ainsi : « *Je ne voudrais effrayer personne, mais il faut se dire que nous n'avons encore rien vu en matière de numérique : la facilité à créer de fausses vidéos très probantes grâce à l'intelligence artificielle, ou encore générer et animer de faux comptes est préoccupante* »¹.

Comme cela a en effet été rappelé *supra* (voir Première partie, IV) été de tels contenus peuvent désormais être produits avec une grande facilité, en quelques minutes et sans débourser un euro.

Le règlement européen sur l'IA apporte un premier élément de réponse, en imposant aux personnes « *qui déploient un système d'IA générant ou manipulant un contenu image, audio ou vidéo constituant une contrefaçon profonde (...) d'indiquer que le contenu a été généré ou manipulé artificiellement* ». En pratique, la Commission européenne a d'ailleurs récemment appelé les grandes plateformes à prendre des mesures pour contrer les risques de manipulations en ligne au moment des élections européennes de juin 2024, visant notamment les contenus générés par l'intelligence artificielle tels que les hypertrucages.

Cependant, comme l'Arcom l'a indiqué au rapporteur, force est de constater que l'*« identification des contenus artificiellement généré ou manipulé pose des questions techniques qui n'ont pas encore été éprouvées »*².

C'est d'autant plus nécessaire que le recours à l'IA générative, qui est propice aux manipulations de l'informations, en particulier dans le cadre d'opérations d'influences étrangères, est susceptible de prendre une part croissante dans les campagnes électorales. À titre d'exemple, un récent rapport de l'organisation non gouvernementale AI Forensics a fait état d'un usage significatif de l'intelligence artificielle dans le contexte des élections législatives françaises de 2024 par certaines formations politiques classées à l'extrême droite (Rassemblement national, Reconquête ! et Les Patriotes), sans jamais indiquer que les publications concernées avaient été générées par l'IA³.

¹ [Audition](#) du 28 mars 2024.

² Réponses de l'Arcom au questionnaire du rapporteur.

³ AI Forensics, [Artifical Elections. Exposing the Use of Generative AI Imagery in the Political Campaigns of the 2024 French Elections](#), 4 juillet 2024

3. La promotion d'une information de qualité : une responsabilité incomptant largement aux médias eux-mêmes, même si l'État peut jouer un rôle d'impulsion et de soutien

a) La définition de méthodologies journalistiques communes

Dans un pays tel que la France, où l'information est libre, la lutte contre les manipulations de l'information dans la sphère médiatique relève avant tout des médias eux-mêmes.

À cet égard, la *Journalism Trust Initiative* (JTI) initiée et déployée par Reporters sans frontières (RSF) doit être soulignée.

Crée en JTI constitue la première et la seule norme internationale pour la fiabilité de l'information. Elle fournit un dispositif transparent pour faire reculer la désinformation et récompenser concrètement le respect d'un journalisme éthique et professionnel. Plus de 1 000 médias dans 85 pays se sont engagés dans la JTI à ce jour en évaluant leurs pratiques, notamment leurs processus éditoriaux. Parmi eux, 250 ont déjà publié leurs rapports de transparence.

Les représentants de RSF auditionnés par la commission d'enquête¹ ont souligné que ce système leur permet non seulement de s'autoévaluer, mais, le cas échéant, d'obtenir le label de la part d'un certificateur indépendant, selon les règles classiques du marché de la certification. Il évalue le respect de 130 indicateurs de méthode. Il est précisé que cette démarche ne concerne en rien le contenu des médias : elle ne porte que sur la méthode. Il s'agit en particulier des exigences de transparence : propriété du média concerné, règles de fonctionnement éditorial ou encore respect de la déontologie professionnelle. Enfin, cette norme a été élaborée sous l'égide du Comité européen de normalisation (CEN). En France, cette mission a ainsi été confié à l'Agence française de normalisation (Afnor).

Il est à noter que le Code européen renforcé de bonnes pratiques contre la désinformation (voir *supra*) s'y réfère expressément.

Selon les représentants de RSF : « *désormais, la norme JTI couvre presque 100 % de l'audience audiovisuelle en France : elle commence à faire autorité* ».

Ils considèrent ainsi que « *à ce jour, les plateformes sont seulement invitées à prendre part à cette amplification des sources fiables d'information. Selon nous, leur participation devrait devenir obligatoire. Ce n'est pas un excès de régulation ou de normativisme, mais une leçon de l'expérience* ».

¹ [Audition](#) du 13 juin 2024.

b) La montée en puissance de la vérification des faits dans les médias français

La commission d'enquête a également souhaité s'intéresser services de vérifications des faits (*fact-checking*) ou de démystification (*debunking*) de plusieurs médias.

En France, le journal Libération a été précurseur en lançant dès 2008 sa rubrique Désintox, devenu CheckNews à compter de 2017, dont la rédactrice en chef adjointe a été auditionnée par la commission d'enquête. Cette rédaction compte aujourd'hui 7 postes à temps plein, à rapporter aux 250 journalistes qui y travaillent. D'autres grands médias français ont lancé une rubrique équivalente en ligne (*Les Décodeurs* du journal Le Monde, *La Vérification*, du journal Le Figaro etc.)

Si ces rubriques n'ont pas vocation à traiter les seules manipulations de l'information relevant d'opérations d'ingérence étrangères, elles peuvent y contribuer. Ainsi, lors de son audition devant la commission d'enquête¹, la rédactrice en chef adjointe de CheckNews a pu revenir sur l'action d'investigation menée en 2023 par sa rédaction concernant l'affaire d'ingérence étrangère à BFMTV, dite « affaire M'Barki », qui a largement été décrite par le rapport de la commission d'enquête de l'Assemblée nationale relatives aux ingérences étrangères².

Les médias français remplissant des missions d'intérêt général mènent une activité importante de vérification des faits, y compris à l'international.

L'Agence France-Presse (AFP) joue à cet égard un rôle clé. Sa direction Investigation numérique emploie 140 journalistes à plein temps, travaillant en 24 langues, couvrant 80 pays et produisant 25 vérifications par jour, ce qui fait du **réseau de l'AFP le plus important au monde en la matière**. Ces vérificateurs peuvent en outre s'appuyer sur l'expertise du réseau global de l'Agence, qui compte 1 700 journalistes dans 151 pays.

Lors de son audition par la commission d'enquête, le directeur Investigation numérique de l'AFP, Grégoire Lemarchand, a relevé que **le rapport de force vis-à-vis des désinformateurs n'en restait pas moins déséquilibré** : « *que la désinformation soit sophistiquée ou non, le combat que nous menons est très inégal : désinformer prend quelques secondes, il suffit d'une capture d'écran et d'un message sur WhatsApp, sans sources, criant au chaos ; en face, nous devons répondre avec des faits, de la nuance et du contexte : cela prend beaucoup plus de temps, a fortiori quand il faut détecter les manipulations, pointer les incohérences*

¹ [Audition](#) du 14 mai 2024.

² [Rapport n° 1311 \(seizième législature\)](#) fait par Constance Le Grip au nom de la commission d'enquête de l'Assemblée nationale relative aux ingérences politiques, économiques et financières de puissances étrangères - États, organisations, entreprises, groupes d'intérêts, personnes privées - visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français, déposé le 1^{er} juin 2023, Tome I.

avec des faits et de la nuance et recouper notre démonstration avec des sources fiables »¹.

Par ailleurs, même si les mentalités évoluent au sein de la profession, il est à noter que la culture de la vérification des faits ne fait pas encore l'unanimité Grégoire Lemarchand ajoute qu'il reste au sein de la profession, même si cela tend à s'amenuiser, une vieille garde qui est un peu réticente ou méprisante à l'égard de notre travail et qui estime que s'occuper de « *deux ou trois zozos pro-russes qui s'agitent sur internet* » n'a pas d'intérêt.

Pour autant, la convention d'objectifs et de moyens (COM) 2024-2028 passée entre l'Agence et l'État souligne la nécessité de poursuivre les efforts en ce sens : *l'investigation numérique « n'est pas une goutte d'eau dans l'océan, comme on l'entend encore trop souvent : les fact-checks atteignent désormais une masse critique, preuve en est qu'il n'est pas une infox significative sur la Covid ou l'Ukraine qui n'ait été contrée ».*

La commission d'enquête relève cependant un point de vigilance concernant le modèle économique de cette activité de l'AFP : celle-ci est essentiellement financée par les plateformes, en tant que clientes de ces investigations numériques dans le souci de montrer publiquement qu'elles luttent contre la désinformation. Ces financements permettent à l'Agence de rendre ces contenus gratuits. Ces ressources provenaient essentiellement de Facebook, mais se sont diversifiées depuis (X, Whatsapp, TikTok), conformément aux orientations prévues par la COM, considérant que cette diversification constitue une garantie d'indépendance. **La COM fixe l'objectif de poursuivre cette diversification au-delà des plateformes**, dont l'engagement à long terme reste incertain comme en témoigne les moyens encore trop limités que celles-ci consacrent à cet enjeu (voir *Troisième partie, III*), en recherchant notamment des financements auprès d'institutions ou de fondations philanthropiques, objectif auquel la commission d'enquête ne peut que souscrire.

Les médias audiovisuels de **France Médias Monde** jouent également, à l'international, un rôle important en la matière. Ses différentes chaînes produisent des contenus de vérifications des faits et de démythification, regroupés sous le label « Stop Infox ». La rubrique « Les Observateurs » de France 24, qui produit ce type de contenus dans les quatre langues de la chaîne (français, anglais, arabe, espagnol), compte 10 ETP mais s'appuie sur un réseau de 5 000 observateurs dans le monde. Plusieurs chaînes RFI sont dotées de rubriques comparables (RFI en persan et RFI en kiswahili notamment).

France Médias Monde s'est également dotée d'une **procédure d'alerte interne**, qui a été communiquée à la commission d'enquête, en cas de manipulations ou d'attaques visant ses médias (voir *Première partie, IV*).

¹ [Audition](#) du 14 mai 2024.

Le groupe enfin **finance des actions de formation des médias locaux** à pour favoriser la production d'une information libre et démocratique au travers de sa filiale CFI, dont le budget était en 2023 de 18,9 millions d'euros.

c) Une structuration de coopérations bienvenues entre médias à l'échelle européenne

La commission d'enquête se félicite de la structuration de coopérations bienvenues entre médias pour le développement de pratiques communes de vérification des faits à l'échelle européenne.

En témoigne la mise en place en 2022, par l'AFP et quatre autres médias spécialisés en Espagne, Pologne, Allemagne et Italie, du *European Fact-Checking Standards Network (EFCSN)*.

Cette organisation a établi un code déontologique de la vérification des faits. Elle vérifie, par des audits, l'indépendance réelle des médias pratiquant la vérification des faits en Europe et leur aspiration aux standards d'objectivité les plus élevés.

Elle compte aujourd'hui 47 membres, dans une trentaine de pays européens, parmi lesquels l'ensemble des États membres de l'Union européenne. Elle se concentre sur la surveillance locale de la désinformation, en fournissant non pas des points de vue abstraits, mais un état actuel des choses. Ses 47 membres fournissent des informations vérifiées et collectent des données sur les contenus, les acteurs, les récits et les formats de désinformation, données ensuite utilisées par presque tous les acteurs de la lutte contre la désinformation, des éducateurs aux grandes plateformes numériques et aux régulateurs et autres autorités publiques. Sa vérification des faits permet de détecter des mensonges et d'enquêter sur eux, dans toutes les langues officielles de l'Union européenne. Nous mettons à la disposition de nos lecteurs des points de contact pour nous alerter.

Son trésorier, Vincent Couronne, a souligné lors de son audition par la commission d'enquête qu' « *un tel réseau est sans précédent dans le monde* »¹.

d) L'Etat peut jouer un rôle d'accompagnement, d'orientation voire d'expertise auprès de ces médias

- (1) Un rôle d'accompagnement et d'orientation des médias réalisant des missions d'intérêt général, qui ne concerne pas spécifiquement la question des ingérences étrangères

Auditionnée par la commission d'enquête, la Directrice générale des médias et des industries culturelles (DGMIC) a indiqué que l'État encourageait, par le biais des conventions d'objectifs et de moyens passés avec les médias réalisant des missions d'intérêt général, les activités de vérification des faits.

¹ [Audition](#) du 14 mai 2024.

Cette activité constitue un « axe prioritaire » de la convention passée à l'AFP. Les conventions passées France Médias Monde et France info intègrent également expressément cet enjeu.

La commission d'enquête relève cependant que ces COM traitent de la lutte contre la désinformation de façon générale, sans aborder la question des ingérences étrangères, alors que celles-ci comportent des problématiques spécifiques et induisent des modes opératoires particuliers, parmi lesquels l'usurpation de l'identité visuelle de ces médias.

S'agissant de la formation des médias locaux, il est à noter que le ministère des affaires étrangères soutient également la filiale CFI de France Médias Monde (mentionnée *supra*) via une dotation financée sur ses crédits à hauteur de 7,2 millions d'euros en 2023.

(2) Avec Viginum, une mise à disposition d'une expertise auprès des médias qui n'a pas encore déployé toutes ses potentialités

Avec Viginum, l'État s'est doté d'une structure capable d'apporter aux médias une expertise spécifique sur les manœuvres d'ingérences numériques étrangères, permettant de mettre à profit ses moyens juridiques exorbitants du droit commun en matière de traitement automatisé de données à caractère personnel dans le cadre de ses investigations en source ouverte¹.

Le travail de ce service est fortement relayé au sein des médias, qui utilisent et commentent largement ses rapports publics.

Suite à sa détection de la campagne *Olympiya* conduite en ligne par des acteurs pro-Azerbaïdjan et visant à discréditer l'organisation des jeux Olympiques et Paralympiques (voir *Première partie, IV*), Viginum avait notamment fait le choix, pour des raisons stratégiques, de ne pas diffuser de rapport public, mais de communiquer à la presse ses analyses techniques, pour laisser le soin aux médias de divulgner l'opération.

4. L'enjeu de l'éducation aux médias et à l'information : une prise en compte insuffisante des influences étrangères malveillantes

La dernière dimension de la politique des médias et de l'information pouvant être mobilisée dans le cadre de la lutte contre les influences étrangères malveillantes concerne **l'éducation aux médias et à l'information (EMI)**.

La loi précitée du 22 décembre 2018 relative à la manipulation de l'information a renforcé les exigences posées par le code de l'éducation en matière d'EMI, notamment en :

- intégrant l'EMI le cadre de l'enseignement moral et civique ;

¹ Décret n° 2021-1587 du 7 décembre 2021 portant autorisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères

- prévoyant expressément que la formation dispensée à tous les élèves des collèges comprend obligatoirement une EMI, intégrant une formation à l'analyse critique de l'information disponible ;
- inscrivant la thématique de l'EMI dans le cadre de la formation des enseignants ;
- prévoyant que les conventions passées entre l'Arcom et les médias audiovisuels puissent comprendre des mesures relatives à l'EMI.

Cependant le constat, ancien, d'un manque **défaut de pilotage** de cette politique a été conforté par une « mission flash » récente de la commission de la culture de l'Assemblée nationale consacrée à cette thématique : « *l'éducation aux médias connaît donc une offre très abondante et émanant d'acteurs divers : nous ne plaidons pas pour son uniformisation, car cette diversité est aussi une richesse, qui permet d'atteindre le public par différents biais ; et quand bien même il y aurait des répétitions, elles peuvent être utiles. Cette offre gagnerait pourtant à être mieux structurée* »¹. La communication relative à cette mission souligne en outre, que **l'offre d'EMI, en dépit de son caractère « pléthorique », est inégalement répartie sur le territoire**.

Le ministère de l'éducation nationale a cependant mené des efforts pour mieux structurer les enseignements apportés dans ce cadre, en lien avec le Centre pour l'éducation aux médias et à l'information (Clemi), qui est indépendant du ministère. Cette impulsion s'est notamment traduite par la publication d'une circulaire visant à généraliser l'EMI², prévoyant notamment la désignation par chaque recteur d'un référent EMI en charge du premier et du second degré, ainsi que la mise à disposition de ressources pédagogiques nationales (guide pratique pour l'EMI).

La démarche est résumée par le directeur général de l'Enseignement scolaire (DGESCO), Edouard Geffray, dans le cadre de son audition par la commission d'enquête : « *notre démarche d'éducation à l'information est plus préventive que curative. Nous ne sommes pas en mesure de déconstruire en classe chaque fausse information qui circule sur les réseaux sociaux. Cependant, notre action court sur toute la scolarité, dès le primaire, sous la forme d'ateliers de sensibilisation. Nos deux approches principales sont les suivantes : la connaissance de la construction de l'information et l'utilisation des médias, et la mise en pratique et la pédagogie des usages, pour que les enfants puissent distinguer ce qui relève du faux et du vrai* »³.

Le Clemi joue un rôle décisif dans le dispositif, en organisant dans les collèges une « semaine de la presse et des médias », qui bénéficie chaque année 4,5 millions d'élèves, soit presque l'intégralité d'entre eux. Ces actions associent des professeurs et des partenaires extérieurs, comme des journalistes

¹ [Communication de la mission flash sur l'éducation critique aux médias, au nom de la commission des affaires culturelles de l'Assemblée nationale](#), par Mme Violette Spillebout et M. Guillaume Ballard, déposé le 15 février 2023.

² Circulaire consultable sur le [site Internet](#) du ministère de l'Éducation nationale.

³ [Audition](#) du 2 mai 2024.

de quotidiens ou de chaînes de télévision, pour que les élèves comprennent comment authentifier une vraie information. Le déploiement de ce type de dispositifs associe l'Arcom, et les acteurs des médias.

L'Arcom a indiqué au rapporteur qu'il veille, depuis 2020, à ajouter une stipulation en matière d'EMI dans les conventions qu'elle signe avec ces dernières. Ainsi, un éditeur est tenu de : « [...] [transmettre] chaque année à l'Arcom des éléments d'information relatifs à son action, ou celle du groupe auquel il appartient, en vue de contribuer à l'éducation aux médias et à l'information ». L'Arcom rend compte chaque année des actions menées dans ce cadre via un rapport *ad hoc*¹.

S'agissant de l'éducation au numérique, le ministère de l'éducation nationale a développé l'outil Pix, qui permet aux élèves de développer des compétences et de bons réflexes numériques – par exemple le fait de ne pas partager des contenus susceptibles de contenir de la désinformation – dès la fin du primaire, avec une attestation délivrée en fin de sixième, généralisée en 2024 à tous les collèges, une certification en fin de troisième et une autre en fin de terminale.

Le DGESCO a précisé lors de son audition que Pix était désormais obligatoire et que Parcoursup demande de plus en plus les attestations afférentes.

En matière de formation des professeurs, le ministère a instauré un plan national de formation, dont l'EMI constitue, selon le DGESCO, « une dimension fondamentale », et qui monte en puissance. Ainsi, en 2021-2022, 393 modules de formation ont été réalisés, pour 4 938 agents formés. En 2022-2023, 359 modules de formation ont été dispensés, à destination de 18 148 agents formés.

Si la commission d'enquête félicite de ces contenus, il ne peut que regretter l'absence de prise en compte de la thématique des manipulations de l'information procédant de stratégies d'influences étrangères malveillantes.

Le guide pratique de l'EMI², publié par le ministère, présente en effet neuf propositions de thématiques à étudier dans le cadre de séquences pédagogiques liées à l'EMI. Parmi elles, aucune ne porte sur les influences étrangères. Il existe bien une thématique « désinformation », dans le cadre de laquelle plusieurs projets éducatifs sont proposés (« comment démêler l'info de l'intox en jouant ? », « décrypter la rhétorique complotiste », « détecter les biais liés aux enjeux environnementaux »). Là encore, le traitement de la question des influences étrangères malveillantes n'est pas proposé.

¹ Arcom, [L'éducation aux médias et à l'information, rapport sur l'exercice 2022-2023](#) (publication la plus récente à date).

² Ministère de l'Éducation nationale, de la Jeunesse et des Sports, [Vademecum Éducation aux médias et à l'information](#).

Cette lacune témoigne d'une forme de naïveté du ministère quant à l'ampleur de cette menace sur l'intégrité de notre espace informationnel, ce qui est d'autant plus regrettable que l'École a un rôle décisif à jouer pour assurer la résilience de la nation face à celle-ci.

En tout état de cause, la commission d'enquête tient à rappeler que si l'EMI a son importance, il ne saurait se substituer à l'exigence de développement de l'esprit critique dès le plus jeune âge, et ce au travers de l'ensemble des enseignements scolaires.

B. LE CONTRÔLE DE LA VIE PUBLIQUE ET POLITIQUE : UN ARSENAL LÉGISLATIF RÉCEMMENT RENFORCÉ, MAIS QUI RESTE À PARFAIRE ET À METTRE PLEINEMENT EN ŒUVRE

1. Le financement des campagnes électorales et de la vie politique : un dispositif de contrôle qui comporte encore certaines failles

Le financement des campagnes électorales et de la vie politique constitue un canal bien identifié pour les opérations d'ingérences à finalité d'influence.

En France, le contrôle du respect par les candidats aux élections et par les formations politiques des règles qui leur sont applicables relève de la Commission nationale des comptes de campagne et des financements politiques (CNCCFP).

Ce corpus juridique, codifié au sein du code électoral, prévoit notamment l'**interdiction de tout concours directs ou indirects au financement des partis en provenance de toute personne morale, française comme étrangère**. Dans le cadre des campagnes électorales, les dons aux candidats ne peuvent qu'être consentis par des personnes physiques (dans la limite de 4 600 euros par personne et par élection) ou des partis politiques.

La loi du 15 septembre 2017 pour la confiance dans la vie politique¹ a porté plusieurs dispositifs importants pour mieux encadrer le recours aux emprunts, en faisant une distinction entre les banques européennes et non-européennes. La loi prévoit ainsi désormais une interdiction générale des prêts de toute personne morale - c'est désormais le principe -, sauf par des partis politiques au sens de la loi du 11 mars 1988² ou par des banques de l'Espace économique européen (EEE). Ainsi, les banques implantées dans les pays n'appartenant pas à cet espace ne peuvent financer de campagnes électorales ni de parti politique. Par ailleurs, des obligations de transparence ont été ajoutées sur ces contrats d'emprunts.

¹ Loi n° 2017-1339 du 15 septembre 2017 pour la confiance dans la vie politique.

² Loi n° 88-227 du 11 mars 1988 relative à la transparence financière de la vie politique.

Cette condition d'appartenance de la banque à l'EEE constitue une garantie importante, en particulier en assurant que celle-ci soit soumise aux règles prudentielles issues des accords de Bâle III.

Par ailleurs, cette loi a prévu une limitation à cinq ans de la durée des prêts des personnes physiques.

Lors de son audition par la commission d'enquête, le Président de la CNCCFP, Jean-Philippe Vachia, a néanmoins indiqué que certains risques et marges d'incertitudes demeurent¹.

La principale marge d'incertitude a trait au « *poids du passé dans les comptes des partis politiques* », avec notamment la question de l'emprunt contracté par le Rassemblement national auprès d'une banque russe en 2014 (voir encadré). Interrogé par le rapporteur sur le point de savoir si ce prêt était assimilable à une ingérence, le président de la CNCCFP a indiqué avoir son « *opinion personnelle* », tout en précisant bien que la CNCCFP « *n'a jamais pris une position qui me permette de répondre positivement* ». En particulier, la commission n'a « *aucun moyen de savoir* » si cet emprunt était assorti ou non de contreparties.

Focus sur l'emprunt contracté par le *Rassemblement national* auprès d'une banque russe en 2014

Le *Front national*, devenu *Rassemblement national* en 2018, avait pu bénéficier en 2014 d'un prêt de plus 9,1 millions d'euros de l'établissement bancaire russe *First Czech Russian Bank*, à échéance 2019. Après sa faillite en 2016, la créance a été reprise par la société russe *Aviazapchast*. Renégociée en 2019 pour, un remboursement par tranches annuelles étalé jusqu'en 2028, cette dette, ayant été contractée sous l'empire des anciennes dispositions applicables avant l'entrée en vigueur au 1^{er} janvier 2018 de la loi du 15 septembre 2017 relative à la confiance de la vie politique, le parti pouvait la conserver au passif de son bilan et continuer à financer ainsi son fonctionnement (avec le relai des emprunts contractés auprès des personnes physiques).

Au 31 décembre 2022 cette dette, en partie amortie depuis 2020, s'élevait encore à 6,5 millions d'euros. Selon les informations communiquées dans la presse, cet emprunt aurait fait l'objet d'un remboursement anticipé en 2023 : l'examen des comptes 2023, à produire avant la date du 30 juin 2024, permettra de le vérifier.

Une fois achevé, le remboursement de l'emprunt souscrit par le *Rassemblement national* en 2014 mettra un terme à la persistance de l'état de fait résultant des dispositions en vigueur avant le 1^{er} janvier 2018.

Source : Rapport annuel 2023 de la CNCCFP

Le président de la CNCCFP en outre a pointé **certaines lacunes importantes qui subsistent dans notre droit**.

¹ [Audition](#) du 28 mars 2024.

En premier lieu, si un critère d'appartenance à l'EEE a été posée pour les banques, aucune règle de nationalité ne vient encadre les prêts consentis par des personnes physiques¹, ni le droit de cotiser auprès d'un parti politique.

De surcroît, le montant de ces prêts des personnes physiques n'est limité par aucun plafond.

Le droit en vigueur ne permet en outre pas d'appréhender certaines activités des candidats et des partis sur les plateformes numériques, et des pratiques éventuelles de rémunérations des créateurs de contenus (ou « influenceurs »), qui peuvent être de nationalité française ou étrangère.

La CNCCFP a fait part à la commission d'enquête de son souhait de disposer de moyens d'enquêtes supplémentaires pour exercer pleinement ses missions.

En particulier, elle propose que lui soient octroyées, pour vérifier l'origine des fonds prêtés ou donnés par les personnes physiques, des prérogatives nouvelles :

- la faculté **d'exiger des preuves auprès des personnes physiques** concernées ;
- la faculté **de saisir Tracfin** pour vérifier la provenance et le circuit des fonds prêtés ;
- la faculté **d'accéder au fichier national des comptes bancaires** (Ficoba).

Ces moyens d'enquêtes sont importants, notamment pour vérifier que la personne physique donnant ou prêtant les fonds n'est pas en réalité intermédiaire qui masquerait un financement prohibé.

2. Les influences étrangères : un « angle mort » du régime de transparence de la vie publique, corrigé par la récente loi visant à prévenir les ingérences étrangères en France

a) Un « angle mort » dans notre dispositif de transparence de la vie publique

Les influences étrangères ont longtemps constitué un « angle mort » du cadre juridique français régissant la transparence de la vie publique, issu principalement des lois organique² et ordinaire³ du 11 octobre 2013 relatives à la transparence de la vie publique, qui a notamment permis la création de la Haute autorité pour la transparence de la vie publique (HATVP).

¹ Il est à noter que les prêts des personnes physiques sont interdits dans le cadre de l'élection présidentielle, mais autorisés pour les autres élections et pour le financement des partis politiques.

² Loi organique n° 2013-906 du 11 octobre 2013 relative à la transparence de la vie publique.

³ Loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique.

Pourtant, comme l'exprime clairement son président Didier Migaud devant la commission d'enquête : « *la multiplication des actions d'influences, directes ou indirectes, exercées par des États étrangers, leur manque de traçabilité, leur complexité font peser des risques importants sur les processus démocratiques nationaux* ». Il ajoute que « *plus la transparence existe sur les actions d'influences étrangères, mieux cela permet d'identifier les mesures d'ingérences étrangères susceptibles d'être conduites par certains pays* »¹.

Jusqu'à la très récente loi visant à prévenir les ingérences étrangères en France (loi « Ingérences étrangères »)(voir encadré), la HATVP n'avait pas pour mandat explicite de contrôler les risques spécifiques liés à des influences étrangères **En pratique, elle ne pouvait apprécier ce risque qu'indirectement, au travers des trois missions principales qu'elle exerce actuellement.**

Premièrement, via la gestion du répertoire des représentants d'intérêts issu de la loi dite « Sapin II »² qui couvre également les représentants d'intérêts étrangers cherchant à influencer les décisions des responsables publics français dès lors qu'ils remplissent les critères enclenchant les obligations déclaratives.

À ce titre, la HATVP avait mis à jour récemment les lignes directrices du répertoire : depuis le 1^{er} octobre 2023, les représentants d'intérêts doivent déclarer les administrations étrangères qui font appel à leurs services. Le bilan de cette évolution est cependant, à ce jour, plutôt décevant, puisque seules deux entités ont déclaré des pays étrangers comme clients :

- *Edile Consulting* qui déclare le Qatar comme client ainsi qu'une fiche d'activité pour son compte ;
- *Espée & Lancée* qui déclare la Corée du Sud comme client.

Ce très faible résultat montre que le dispositif d'encadrement de la représentation d'intérêts en France issu de la loi Sapin II n'est pas adapté – car trop restrictif – pour permettre de tracer efficacement les activités d'influence étrangère.

Deuxièmement, via le contrôle des mobilités professionnelles des responsables publics entre les secteurs public et privé, qui peut porter sur les carrières de hauts fonctionnaires français établis à l'étranger ou des responsables publics qui souhaitent rejoindre des entreprises étrangères. Néanmoins, la prise en compte de risques liés à une influence étrangère se heurte à une limite juridique : dans le cadre de son mandat, la Haute Autorité peut éventuellement identifier un tel risque mais son contrôle, conformément à la loi, vise exclusivement à prévenir les risques d'ordre pénal et déontologique.

¹ [Audition](#) du 23 mai 2024.

² Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Troisièmement, via le contrôle des déclarations d'intérêts déposées par les responsables publics. Ce contrôle peut permettre, le cas échéant, à la Haute Autorité d'identifier l'existence de certaines associations très liées à des États étrangers dans lesquelles les déclarants auraient des fonctions dirigeantes ou rémunérées.

La loi visant à prévenir les ingérences étrangères en France

La loi visant à prévenir les ingérences étrangères en France, définitivement adoptée au Parlement le 5 juin 2024, est issue d'une proposition de loi des députés Sacha Houlié, Constance Le Grip et Thomas Gassilloud. Elle fait suite aux rapports de la commission d'enquête de l'Assemblée nationale relative aux ingérences étrangères¹, ainsi qu'au rapport annuel 2022-2023 de la délégation parlementaire au renseignement, qui était pour partie consacré à cette même question².

Son article 1^{er} institue un répertoire national des représentants d'intérêts agissant pour le compte de mandants étrangers sur le modèle du *Foreign Agents Registration Act* (FARA) états-unien, géré par la Haute autorité pour la transparence de la vie publique (HATVP).

Son **article 2** prévoit un contrôle de la même HATVP sur les **risques d'influence étrangère en matière de reconversion professionnelle** des responsables publics dans le secteur privé.

Son **article 3** prévoit une obligation de transmission à la HATVP des informations relatives aux **financements étrangers perçus par les laboratoires d'idées (think tanks)**.

Son **article 4** prévoit la remise par le Gouvernement au Parlement d'un **rapport biannuel sur l'état des menaces** qui pèsent sur la sécurité nationale, en particulier celles résultant d'ingérences étrangères.

Son **article 5** permet de renforcer le contrôle parlementaire en matière de sécurité économique, en précisant que la publication annuelle des données statistiques relatives au contrôle par le Gouvernement des investissements étrangers en France puisse donner lieu à un débat dans les assemblées.

Son **article 6** autorise les services de renseignements, à titre expérimental jusqu'au 1^{er} juillet 2028, à utiliser la technique consistant à faire fonctionner des traitements automatisés de données (technique dite « de l'algorithme), dans le but détecter des connexions susceptibles de révéler toute forme d'ingérence ou de tentative d'ingérence étrangère. Cette technique était jusqu'ici réservée aux seuls besoins de la prévention du terrorisme

Son **article 7** ouvre au ministre chargé de l'économie et au ministre de l'intérieur la possibilité de décider, conjointement, le gel des fonds et ressources économiques des

¹ [Rapport n° 1311 \(seizième législature\)](#) fait par Constance Le Grip au nom de la commission d'enquête de l'Assemblée nationale relative aux ingérences politiques, économiques et financières de puissances étrangères – États, organisations, entreprises, groupes d'intérêts, personnes privées – visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français, déposé le 1^{er} juin 2023.

² *Rapport public n° 1454 (seizième législature- Assemblée nationale) / n° 810 (2022-2023 – Sénat)* fait par Sacha Houlié au nom de la délégation parlementaire au renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023, déposé le 29 juin 2023.

personnes physiques ou morales ou de toute autre entité qui commettent, tentent de commettre, facilitent ou financent des actes d'ingérence, y incitent ou y participent.

Son **article 8** prévoit une aggravation des peines encourues en cas d'infraction pénale commise pour le compte d'une entité étrangère et à autoriser, dans le cadre de la judiciarisation de telles infractions, le recours aux techniques spéciales d'enquête prévues notamment en matière de criminalité organisée (interceptions de correspondances, surveillance, infiltration, recueil de données de connexion, captation de données...).

Son **article 9** porte sur l'application de la loi dans les Outre-mer.

Source : commission d'enquête

b) La loi visant à prévenir les ingérences étrangères a permis de combler certaines lacunes

La loi « Ingérences étrangères » en France a prévu trois dispositifs bienvenus pour combler cette lacune, en confiant à la HATVP trois nouvelles missions spécifiques.

(1) La création d'un « FARA » à la française

En premier lieu, l'article 1^{er} de cette loi vient créer un répertoire national des représentants d'intérêts agissant pour le compte de mandants étrangers sur le modèle du *Foreign Agents Registration Act* (FARA) états-unien (voir encadré), géré par la Haute autorité pour la transparence de la vie publique (HATVP).

La France s'inscrit ainsi dans le sillage d'autre pays de l'OCDE ayant mis en place un dispositif similaire : l'Australie dès 2018, avec le *Foreign Influence Transparency Scheme (FITS) Act* de 2018 et le Royaume-Uni, qui est en train d'établir également le *Foreign Influence Registration Scheme (FIRS)* à la suite de la mise à jour de la loi sur la sécurité nationale en 2023.

DOCUMENT PROVISOIRE

Le *Foreign Agents Registration Act* (FARA) aux États-Unis

La loi américaine sur l'enregistrement des agents étrangers (22 U.S.C. §§611-621 ; « *Foreign Agents Registration Act* » - FARA) a été promulguée en 1938 dans un contexte d'influence grandissante de la propagande nazie aux États-Unis. Dans les années précédant la Seconde Guerre mondiale, le Congrès américain avait en effet identifié plusieurs personnes et organisations opérant aux États-Unis et propagant de la propagande ayant pour but de façonnner l'opinion publique américaine en donnant une image positive du nouvel État allemand et en contrant certains rapports faisant état de la brutalité du régime nazi à l'égard des opposants politiques et des Juifs.

Sur recommandation de la commission spéciale sur les activités anti-américaines du 73^{ème} Congrès (1934-1935), l'adoption du FARA avait donc pour objectif de faire la lumière sur l'utilisation de « *proxies* » en exigeant plutôt que les personnes engagées dans des activités de propagande pour le compte de gouvernements étrangers s'enregistrent auprès du gouvernement et rendent transparentes des informations sur leurs clients, leurs activités et les termes de leurs contrats, sans toutefois interdire ces activités. À cet égard, le FARA est souvent considéré comme la loi sur le *lobbying* la plus ancienne du monde.

Amendé au fil des ans, le FARA s'applique aujourd'hui largement à toute personne qui agit au nom d'un mandant étranger (« *foreign principal* ») pour, entre autres, influencer la politique ou l'opinion publique des États-Unis.

Concrètement, le FARA exige de certains agents qui mènent certaines activités d'influence pour le compte d'entités étrangères (*foreign principals*) d'enregistrer périodiquement auprès du département de la Justice (*Department of Justice*) leurs relations avec le mandant étranger, ainsi que les activités et dépenses à l'appui de cette influence. Le département de la Justice est tenu de rendre ces informations accessibles au public.

Source : OCDE « *Renforcer la transparence et l'intégrité des activités d'influence étrangère en France* », 2024.

Concrètement, le dispositif prévu par la loi « Ingérences étrangères » en France prévoit la tenue par la HATVP d'un répertoire spécifiquement aux activités d'influence réalisées pour le compte d'un mandant étranger, distinct de celui prévu par la loi Sapin II. Celui-ci entrerait pleinement en vigueur à compter du **1^{er} juillet 2025**.

Selon les termes de cette loi, sont visées toutes les activités des représentants d'intérêt agissant pour le compte d'un mandant étranger et qui destinées à influer sur la décision publique, notamment sur le contenu d'une loi, d'un acte réglementaire ou d'une décision individuelle, ou sur la conduite des politiques publiques nationales et de la politique européenne ou étrangère de la France. Les **activités concernées** sont ainsi celles consistant à :

- entrer en communication avec les principaux responsables publics ou leurs collaborateurs : les membres (ou anciens membres) du Gouvernement ou de cabinets ministériels, les parlementaires (ou anciens parlementaires) et leurs collaborateurs, les anciens présidents de la République, les collaborateurs du président de la République, les responsables d'autorités indépendantes, les élus des collectivités territoriales de plus de 20 000 habitants, les candidats déclarés aux élections nationales, les dirigeants de partis, certains hauts fonctionnaires *etc.* ;

- réaliser toute action de communication à destination du public ;
- collecter des fonds ou procéder au versement de fonds sans contrepartie.

Les déclarations doivent porter sur :

- l'identité du représentant d'intérêt et du mandant étranger ;
- le contenu de l'accord ou la nature du lien entre la personne agissant pour le compte d'un mandant étranger et le mandant étranger - la loi étant rédigée ici de façon volontairement souple, de telle sorte que l'absence de contrat officiel ne permette pas de contourner l'obligation de déclaration ;
- le nombre de personnes employées dans l'accomplissement des activités concernées et, le cas échéant, le chiffre d'affaires généré par ces activités durant l'année précédente ;
- le détail des actions réalisées.

Le dispositif prévoit également certaines obligations régissant les représentants d'intérêts, en prévoyant expressément, lorsqu'ils entrent en communication avec un responsable public, qu'ils :

- déclarent leur identité ;
- s'abstiennent de leur offrir des présents, des dons ou des avantages quelconques d'une valeur significative ;
- s'abstiennent de toute incitation à l'égard de ces personnes à enfreindre les règles déontologiques qui leur sont applicables

Enfin, il octroie à la HATVP certaines prérogatives spécifiques pour contrôler le respect de ces nouvelles dispositions. Cette dernière peut ainsi :

- à son initiative ou à la suite d'un signalement, mettre en demeure toute personne à l'égard de laquelle il existe des raisons sérieuses de penser qu'elle entre dans le champ des personnes soumises à déclaration de lui communiquer, dans un délai d'un mois, toute information ou tout document nécessaire à l'exercice de sa mission, sans que le secret professionnel puisse lui être opposé ;

DUPOVINE

- procéder à des vérifications sur place dans les locaux professionnels de ces personnes, sur autorisation du juge des libertés et de la détention du tribunal judiciaire de Paris et en présence d'un officier de police judiciaire, lors desquelles ses agents peuvent exiger la communication et obtenir ou prendre copie, par tout moyen et sur tout support, des documents professionnels de toute nature, entre quelques mains qu'ils se trouvent, propres à faciliter l'accomplissement de leur mission ;

- demander aux responsables publics visés par le texte la liste des représentants d'intérêts agissant pour le compte de mandants étrangers entrés en communication avec eux ;

Lorsqu'elle constate un manquement aux règles prévues, la HATVP peut :

- mettre la personne concernée en demeure de respecter ces obligations, et éventuellement rendre publique cette mise en demeure ;
- si la mise en demeure n'est pas suivie d'effet, prononcer une astreinte dont le montant maximal est fixé à 1 000 euros par jour, et qu'elle peut rendre publique.

Enfin, la loi crée un nouveau **délit** constitué par le fait pour une personne de se soustraire à ses obligations déclaratives, et puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

La commission d'enquête ne peut que saluer la mise en place de ce dispositif, qui constitue une avancée réelle.

(2) Un contrôle des mobilités professionnelles des responsables publics à l'aune du risque d'influence étrangère

L'article 2 de cette même loi permet également de **renforcer le mandat de la HATVP pour lui permettre de prendre en compte les risques d'influence étrangère dans le cadre de son contrôle des reconversions professionnelles dans le secteur privé des hauts responsables publics.**

Sont concernés les personnes ayant exercé, au cours des cinq dernières années :

- des fonctions gouvernementales ;
- des fonctions de membre d'une autorité administrative indépendante ou d'une autorité publique indépendante ;
- des fonctions exécutives au sein d'une collectivité locale de plus de 20 000 habitants.

Dans ce cadre, la HATVP se prononce sur la compatibilité de l'exercice de l'activité privée concernée avec les fonctions précitées. En cas d'avis d'incompatibilité, la personne concernée ne peut pas exercer l'activité envisagée pendant une période épurant trois ans après la fin de l'exercice des fonctions.

Cette mesure, qui constitue un apport du Sénat lors de l'examen du texte, est également de bon sens.

(3) Un contrôle du financement des laboratoires d'idées

Enfin, l'article 3 de la même loi crée une **obligation nouvelle pour les laboratoires d'idées (think tanks) de transmettre à la HATVP le montant des dons et versements étrangers qu'ils reçoivent.**

S'il est bien légitime, pour un État, de mener une politique d'influence consistant à peser sur les débats publics étrangers dans le sens de ses intérêts, une telle politique doit être menée à visage découvert, sans quoi elle relève

purement et simplement de l'ingérence. **Ce dispositif constitue ainsi une garantie de transparence du débat public** à cet égard.

c) *Un manque de moyens avéré pour la HATVP*

La principale question qui se pose est désormais celle de l'adéquation entre les exigences de bonne application de ces dispositifs et les moyens dont cette institution dispose effectivement.

La création du nouveau répertoire des représentants d'intérêts agissant pour le compte de mandants étrangers suppose notamment, en effet, comme l'a précisé le Président Didier Migaud lors de son audition, de créer de nouveaux logiciels et des nouvelles applications informatiques.

Pour Didier Migaud, les moyens actuels de la HATVP, qui sont déjà taillés au plus juste sont largement insuffisants pour accomplir ces nouvelles missions : « *en termes de moyens, la Haute Autorité dispose aujourd'hui de 75 agents. Une dizaine de personnes sont affectées au contrôle du répertoire des représentants d'intérêts au titre de la loi Sapin II : la comparaison de nos moyens avec des pays ayant mis en place des obligations et répertoires similaires m'inspire une certaine gêne, tant ces effectifs sont insuffisants. Nous manquons donc déjà de personnel pour faire vivre ce répertoire et procéder aux contrôles requis, avant la mise en place de tout autre dispositif* »¹.

Il s'agit donc, pour la commission d'enquête, d'un point de vigilance majeure dans la perspective des prochains débats budgétaires.

C. L'ENSEIGNEMENT SUPÉRIEUR ET LA RECHERCHE : UNE MISE EN ŒUVRE ENCORE INCOMPLÈTE DES RECOMMANDATIONS DU RAPPORT « GATTOLIN »

1. La prise de conscience par le ministère d'un risque d'influences étrangères bien réel

a) *L'enseignement supérieur et la recherche, un secteur particulièrement exposé au risque d'influences étrangères*

Comme cela a été bien mis en évidence par le rapport fait par André Gattolin au nom de la mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences (« rapport Gattolin »)² et rappelé par le présent rapport (voir *Première partie, I*), **le secteur de l'enseignement supérieur et de la recherche est particulièrement exposé aux influences étrangères**.

¹ [Audition](#) du 23 mai 2024

² [Rapport d'information n° 873 \(2020-2021\)](#) fait par André Gattolin au nom de la mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences, déposé le 29 septembre 2021.

Le « rapport Gattolin » distingue cinq modes d'action principaux des opérations d'influence étatiques ciblant l'université :

-la **diplomatie d'influence**, qui se traduit notamment par la promotion de l'enseignement d'une langue, l'organisation de manifestations culturelles, mais aussi par des liens tissés dans le domaine économique. La Chine est particulièrement active dans ce domaine, au travers des centaines « **Instituts Confucius** » ouverts dans le monde (plus de 500 dénombrés) ;

- les relations directes entre les États et les universités, qui peut passer par le financement d'établissements (plus rare en France où celui-ci est davantage public qu'ailleurs), ainsi que par les pressions pouvant être exercées par les étudiants ressortissants de cet état au sein de l'université ;

- l'interdépendance tissée dans la recherche, qui explique notamment la volonté des acteurs chinois de nouer des partenariats avec des unités de recherche spécialisées dans des segments technologiques pour lesquelles l'économie chinoise dépend encore de l'extérieur ;

- des méthodes plus coercitives, qui peuvent prendre des formes variées : recours devant les tribunaux, espionnage et pillage de technologies, restrictions d'accès faites aux chercheurs souhaitant mener des recherches dans l'État concerné, pouvant aller jusqu'au refus de visa ;

- la **diplomatie publique** au travers du financement de structures se trouvant à la frontière de la recherche, notamment les laboratoires d'idées (*think tanks*), afin que ceux-ci portent des narratifs favorables l'État financeur. À cet égard, le rapport pointe en particulier l'action d'États du Golfe (Qatar, Émirats arabes unis, Arabie saoudite) ainsi que de la Chine. La commission d'enquête relève que la mesure de transparence adoptée à cet égard dans le cadre de la loi « Ingérences étrangères », rappelée *supra*, répond en partie à cette problématique.

Cette action d'influence procède de quatre objectifs :

- se constituer des aires géographiques d'influence : peuvent à cet égard être mentionnés les 62 Instituts Confucius dénombrés de 45 pays différents en Afrique¹ ;

- contrôler les diasporas ;

- contrôler les normes d'impulsion de la recherche, le rapport Gattolin relevant que la Chine mène une stratégie ambitieuse d'influence sur la production de normes, qui passe par une action au niveau des organisations internationales compétentes, mais également par le fait de peser dans les programmes d'évaluation internationaux, à l'instar du classement de Shanghai qui cherche à évaluer les établissements d'enseignement supérieur

¹ Selon les chiffres donnés par le [site officiel](#) des Instituts Confucius.

sur leur mérite scientifique, qualifié de « grande réussite de la politique d'influence académique de la Chine » ;

- défendre un modèle de société. Le rapport rattache cette stratégie à la diplomatie publique d'acteurs tels que la Turquie et la Chine : « *au niveau académique, cette volonté de remettre les pays émergents au cœur du jeu international passe par la promotion de valeurs substitutives, qui se définissent en opposition aux valeurs des démocraties libérales* »

La commission d'enquête tient à souligner que l'exposition des universités françaises aux influences étrangères n'est que la résultante et l'illustration du « désarmement de l'État ». Les sous-financements constatés de façon récurrentes sur certains secteurs de la recherche constituent une brèche dans laquelle s'engouffrent les opérations d'influence. Lors de leur audition par le rapporteur, les responsables de l'Institut national des langues et des cultures orientales (Inalco) ont notamment pris l'exemple de l'action de l'entreprise chinoise Huawei, qui a proposé des bourses de doctorat en faveur de recherches en traitement automatique des langues (TAL).

b) Une prise de conscience affichée par les responsables du ministère

Les principaux responsables du ministère de l'Enseignement supérieur et de la recherche auditionnés par la commission d'enquête ont tenu à affirmer leur **prise de conscience du phénomène**.

La ministre, Sylvie Retailleau, a ainsi pu souligner que « *les actes malveillants émanant de puissances étrangères sont incontestablement un enjeu crucial, qui interdisent toute naïveté et nécessitent une forte vigilance* ». Elle a fait état d'une « *prise en compte accrue des enjeux de sécurité dans mon ministère, et ce pour plusieurs raisons : d'abord, un cadre géopolitique instable, avec la guerre en Ukraine, le conflit au Proche-Orient, les prétentions hégémoniques de diverses puissances, dont certaines mènent des entreprises de captation, et l'accroissement des tensions liées aux velléités de prolifération ; ensuite, une conflictualité accrue et une montée en puissance des rapports de force dans les mouvements sociaux, particulièrement dans les universités ; enfin, un contexte général de montée des menaces et des violences aux personnes* »¹.

S'agissant spécifiquement des **Instituts Confucius**, la Ministre a indiqué lors de son audition que ceux-ci « *font l'objet d'une vigilance très particulière, notamment depuis le rapport d'information rédigé par André Gattolin en 2021. Chaque situation fait l'objet d'un suivi au cas par cas, en lien avec le SGDSN et les établissements. Par principe, nous demandons que les instituts disposent d'une personnalité juridique propre et qu'ils ne soient pas adossés aux établissements. Toutefois, par exception, nous acceptons qu'un tel institut soit intégré à un établissement lorsque la convention est de nature à assurer un meilleur contrôle avec un système d'information séparé, des locaux éloignés des laboratoires de recherche sensibles, etc. Nous ne sommes pas opposés, par principe, à la présence des instituts Confucius en France. Nous veillons toutefois à ce que l'activité de tels instituts se*

¹ [Audition](#) du 18 juin 2024.

cantonne au domaine de la linguistique. Nous ne pouvons pas tolérer une influence dans d'autres champs d'activité de nos établissements d'enseignement supérieur, tels que les choix et méthodes pédagogiques, ou le contenu des enseignements ».

Dans les réponses au questionnaire du rapporteur, le secrétaire général du ministère de l'éducation nationale et de la jeunesse, du ministère de l'enseignement supérieur et de la recherche et du ministère des sports et des jeux Olympiques et Paralympiques Thierry Le Goff, auditionné en sa qualité de haut fonctionnaire de défense et de sécurité (HFDS) pour ces ministères, affirme également que : « *le ministère de l'enseignement supérieur et de la recherche exerce une vigilance particulière, sans naïveté, sur les opérations d'influence étrangères dans les établissements* ». Il précise en outre que : « *la menace est protéiforme et émane principalement d'acteurs étatiques identifiés (Chine, Russie, Turquie)* ».

Lors de son audition, l'adjoint à la directrice générale de l'enseignement supérieur et de l'insertion professionnelle (DGESIP), Benjamin Leperchey, a étendu la cartographie de l'origine des menaces, indiquant que « *les usual suspects sont la Chine, la Russie depuis quelques années, l'Afrique du Nord, beaucoup, et un peu moins le Moyen-Orient, la Turquie ou l'Azerbaïdjan. Les premiers pays cités sont les plus directement intrusifs* ». Invité par le rapporteur à préciser son propos sur les actions émanant d'Afrique du Nord, l'action du Maroc a été citée¹.

Compte tenu de l'actualité récente, plusieurs membres de la commission d'enquête se sont interrogés sur le lien possible entre des opérations d'influence étrangères et les récentes manifestations étudiantes propalestiniennes, lancées dans le contexte du conflit en cours à Gaza. Sur ce point, la Ministre Sylvie Retailleau a indiqué à la commission d'enquête que : « *nous ne méconnaissons pas ce que j'appellerai les rumeurs qui existent au sujet d'opérations d'influence étrangère à l'œuvre dans des actions menées depuis quelques mois dans les campus universitaires à propos du conflit israélo-palestinien. Pour autant, à ma connaissance, aucun lien n'a été établi dans aucun établissement d'enseignement supérieur et de recherche entre de tels mouvements et des puissances étrangères déterminées* ».

2. Un dispositif de protection qui repose sur l'action du service de défense et de sécurité du ministère et le volontarisme des établissements, qui n'est pas encore à la hauteur de la menace

a) Un dispositif qui s'inscrit dans les grands principes régissant l'université et sa gouvernance

La lutte contre les influences étrangères dans le domaine de l'enseignement supérieur et la recherche s'inscrit nécessairement dans le cadre des grands principes qui régissent l'université et sa gouvernance.

¹ [Audition](#) du 2 mai 2024.

En premier lieu, toute mesure de protection doit être conciliée avec le respect des libertés académiques, qui sont consacrées par la loi¹ et qui sont au fondement même de l'université. L'ouverture au monde extérieur, par la voie d'échanges entre établissements, étudiants et chercheurs, est un élément naturel de leur exercice. Dans le même temps, il convient de noter que des influences étrangères malveillantes ou dissimulées, empruntant la voie de l'ingérence, constituent en réalité des menaces pour le plein exercice des libertés académique, et partant que la protection contre celles-ci concourt à les préserver.

En second lieu, le dispositif de protection doit s'articuler avec le principe d'autonomie de gestion des universités, qui rend le chef d'établissement responsable de la politique de défense et de sécurité.

b) Au niveau du ministère, la lutte contre les influences étrangères relève de la compétence du service de défense et de sécurité

(1) Le service de défense et de sécurité : un service qui monte en puissance, mais dont les moyens restent insuffisants

Le service de défense et de sécurité (SDS) est placé sous la responsabilité du secrétaire général du ministère de l'éducation nationale et de la jeunesse, du ministère de l'enseignement supérieur et de la recherche et du ministère des sports et des jeux Olympiques et Paralympiques en sa qualité de HFDS.

Il est compétent sur le périmètre de ces trois ministères. Le SDS exerce une mission d'animation et de coordination de la politique de sécurité et de défense (conception de plans, conception et diffusion de plans, veille et alerte, protection des biens et des personnes, protection du potentiel scientifique et technique, protection du secret, sécurité des systèmes d'information, intelligence économique) en lien avec tous les services de l'État, notamment le SGDSN et les services de renseignement.

En revanche, il ne mène pas de missions d'enquête, de police ou de renseignement, qui relève des ministères de l'intérieur et de la justice.

Le SDS est structuré en sept pôles, dont aucun n'est spécifiquement dédié à la lutte contre les influences étrangères². Pour mener ses missions, il s'appuie sur un réseau de 143 fonctionnaires de sécurité et de défense (FSD) en poste dans les universités, auprès des présidents.

Le plafond d'emploi de ce service s'élève à 44 équivalents temps plein (ETP) en 2024, soit un total en nette augmentation au cours des dernières années (+ 23 ETP par rapport à 2017). Si une telle augmentation des effectifs

¹ Article L. 952-2 du code de l'éducation.

² Les sept pôles concernent : la protection du potentiel scientifique et technique de la Nation (PPST) ; la protection du secret de défense nationale ; la cellule ministérielle de veille et d'alerte, la planification et la gestion de crise ; la sécurité des systèmes d'information ; les valeurs de l'École de la République et l'administration générale du SDS.

traduit bien une prise de conscience accrue des enjeux de sécurité, le secrétaire général considère que le service n'a pas encore atteint sa « taille critique » eu égard à l'ampleur des besoins, ce d'autant plus que 13 postes ne sont pas pourvus à date. Les besoins supplémentaires sont évalués à 11 ETP supplémentaires au sein du SDS. Au sein du réseau, le besoin de FSD est quant à lui évalué à 140 ETP, soit un doublement. Selon les informations communiquées par le HFDS, ces besoins ont été soumis à un arbitrage budgétaire interministériel.

Au-delà du renforcement de ses effectifs, une professionnalisation du réseau est nécessaire, les FSD cumulant bien souvent cette fonction avec d'autres fonctions administratives.

Alors qu'une réorganisation complète du SDS est envisagé dans le cadre de cette montée en puissance, **la commission d'enquête relève que celle-ci serait l'occasion de mieux prendre en compte, dans son organisation, la problématique croissante des influences étrangères.**

(2) Le dispositif de protection du patrimoine scientifique et technique de la Nation n'est pas pleinement adapté à la menace liée aux influences étrangères

L'une des activités majeures du SDS concerne la **protection du patrimoine scientifique et technique (PPST)** de la Nation, qui peut être ciblé dans le cadre d'opération d'ingérences étrangères. La mise en œuvre de ce dispositif implique une procédure très encadrée visant à définir des **zones à régime restrictif (ZRR)**, c'est-à-dire des zones d'accès restreint au sein même de l'université, dans les unités de recherche, pour limiter l'accès à des domaines jugés sensibles. Le fait de s'introduire sans autorisation dans une ZRR est caractérisé au plan pénal comme une atteinte aux intérêts fondamentaux de la Nation et constitue un délit puni de six mois d'emprisonnement et de 7 500 euros d'amende.

Il existe aujourd'hui **931 ZRR** (dont 201 créées en 2023), réparties dans 66 établissements. Environ 38 000 personnes y ont accès. Au total, **17 843 demandes d'accès** ont été examinées en 2023, faisant systématiquement l'objet d'une instruction par la DGSI. Parmi elles, **470 demandes ont été refusées**. La Ministre Sylvie Retailleau, lors de son audition, a précisé que : « *Pour les États les plus sensibles, le nombre d'avis réservés et défavorables a dépassé le nombre d'avis favorables* ». Le détail des refus d'accès en fonction des pays d'origine n'a cependant pas été communiqué à la commission d'enquête, au motif qu'il serait couvert par le secret de la défense nationale.

Cependant, le dispositif n'est aujourd'hui pas pleinement adapté aux enjeux de la lutte contre les influences étrangères. En ce qu'il vise avant tout à prévenir le risque d'une captation de savoirs, de savoir-faire et de technologies sensibles à des fins économiques et industriels, celui-ci concerne avant tout les sciences dites « dures », et non les sciences humaines et sociales.

Pourtant, les sciences humaines et sociales constituent bien, comme l'avait souligné le rapport Gattolin précité, le cœur de cible des stratégies d'influence *stricto sensu*, qui « entendent influer sur les travaux de chercheurs afin d'imposer une vision plus positive de leur modèle, de limiter l'expression académique ou de promouvoir leur doctrine sur certains sujets jugés sensibles, comme par exemple les Ouïghours en Chine ».

L'exclusion des sciences humaines et sociales du champ des PPST témoigne ainsi d'une conception restrictive des intérêts fondamentaux de la Nation, eu égard au durcissement des opérations d'influence à l'œuvre au cours des dernières décennies.

Il est cependant à noter que ce dispositif est en cours de réforme, avec la parution récente d'un décret du 14 mai 2024¹ qui en renforce la portée sur plusieurs points significatifs à compter du 1^{er} janvier 2024 (voir encadré).

DOCUMENT PROVISOIRE

¹ Décret n° 2024-430 du 14 mai 2024 portant diverses dispositions relatives à la protection du potentiel scientifique et technique de la Nation.

Principaux éléments introduits par le décret n° 2024-430 du 14 mai 2024 portant diverses dispositions relatives à la protection du potentiel scientifique et technique de la Nation

L'entrée en vigueur du décret n° 2024-430 du 14 mai 2024 portant diverses dispositions relatives à la protection du potentiel scientifique et technique de la Nation (PPST) est fixée au 1^{er} janvier 2025.

Ce décret porte principalement les évolutions suivantes :

- il introduit un régime contraventionnel (amende de 5^{ème} catégorie) qui cible, d'une part, les manquements aux obligations de protection et de mise en œuvre d'une zone à régime restrictif (ZRR) et, d'autre part, le fait de faire obstacle à l'accomplissement des missions des personnels chargés de la protection des ZRR.

- Une contravention de 5^{ème} catégorie pourra être adressée à un établissement de l'enseignement supérieur et de la recherche, relevant des dispositions du code de l'éducation (article L. 123-7-1), ne respectant pas l'obligation d'information des ministères d'un projet d'accord international impliquant des activités conduites au sein d'une ZRR. Cette disposition vient donc renforcer la portée de la circulaire du ministère de l'Enseignement supérieur et de la Recherche du 18 janvier 2022 sur les modalités de communication préalable des projets d'accords internationaux des établissements de l'enseignement supérieur et de la recherche.

- toutes les personnes qui bénéficient d'un avis favorable pour l'accès à une zone à régime restrictif afin d'y exercer des activités d'entretien, de gardiennage, de soutien aux activités de recherche (sauf pour les services informatiques) bénéficient d'un avis favorable pour l'accès, aux mêmes fins et dans les mêmes limites, aux autres zones à régime restrictif relevant du même ministre.

- le ministre peut, de sa propre initiative et à tout moment, revenir sur le sens de son avis, y compris lorsque celui-ci est réputé favorable, comme c'est le cas par exemple pour les personnels en place au sein d'une ZRR au moment de sa création (point non prévu actuellement).

- le silence gardé dans un délai de deux mois par le ministère après la réception de la demande d'avis formulée par l'établissement, vaut avis défavorable implicite (il est implicitement favorable aujourd'hui).

- le silence gardé par le chef d'établissement dans un délai de trois mois (deux mois aujourd'hui) suivant la réception par celui-ci d'une demande d'autorisation d'accès vaut décision de rejet.

- le bénéficiaire d'une autorisation d'accès à une ZRR est tenu d'informer le chef d'établissement de tout changement de situation susceptible d'affecter l'appréciation portée sur son droit d'accès. Le chef d'établissement doit en informer sans délai le ministre.

Source : Haut fonctionnaire de défense et de sécurité du ministère de l'Enseignement supérieur et de la Recherche

(3) Un dispositif de détection des influences étrangères insuffisant et mal adapté

Les travaux de la commission d'enquête ont mis en évidence la difficulté pour le ministère à recenser les situations et problématiques liées à des ingérences potentielles.

Lors de son audition devant la commission d'enquête, la ministre Sylvie Retailleau a souligné les difficultés rencontrées par le ministère pour détecter les situations problématiques : « *le caractère insidieux de ces démarches peut rendre compliquée leur détection. Il n'existe pas de recensement et de suivi exhaustif de ces situations au sein du ministère, car c'est une compétence de la direction générale de la sécurité intérieure (DGSI), mais des axes de travail permettent de disposer de remontées d'incidents, sans que celles-ci aient un caractère obligatoire : je pense par exemple à l'ouverture de la cellule ministérielle de veille et d'alerte (CMVA) aux établissements d'enseignement supérieur et de recherche* »¹.

Dans ses réponses au questionnaire du rapporteur, le HFDS ajoute que « *l'autonomie de gestion des universités, qui rend le chef d'établissement responsable de la politique de défense et de sécurité, et le principe fondamental de liberté académique font, pour l'heure, obstacle à un recensement et un suivi exhaustif des situations* ».

Pour la commission d'enquête, ces réponses ne sauraient être jugées satisfaisantes.

En premier lieu, si le travail d'enquête, de caractérisation et le cas échéant d'entrave relève bien de la DGSI, il appartient au ministère et aux universités de se doter de capteurs adéquats pour faire remonter les situations suspectes aux services de renseignement, qui ne peuvent pas surveiller en permanence chaque université.

En deuxième lieu, la cellule ministérielle de veille et d'alerte (CMVA) n'est aujourd'hui pas outillée pour recenser ces situations.

Gérée par le SDS, cette cellule centralise les incidents survenus dans les écoles et les universités et fonctionne en permanence.

Le rapporteur a sollicité le HFDS pour obtenir le détail des signalements effectués, qui s'élèvent à 620 entre septembre 2023 et mai 2024. Cela étant, ces éléments sont peu probants pour la commission d'enquête, en ce qu'ils ne permettent pas d'identifier les signalements liés à une influence étrangère. Comme l'indique le HFDS : « *aucune typologie ne permet, à ce stade, de mettre particulièrement en exergue les opérations d'influences étrangères* ». En effet, le système de signalement repose à ce jour sur les seules catégories suivantes : mouvements sociaux (59 % des signalements), atteintes aux personnes (13 %), atteintes aux valeurs de la République (12 %), atteintes à la sécurité ou au climat (11 %), décès (4 %) et atteintes aux biens (1 %).

¹ [Audition](#) du 18 juin 2024.

Dans ses réponses, le HFDS annonce des évolutions en ce sens, auxquelles il conviendra donc de veiller : « *la catégorisation des incidents, qui doit pouvoir permettre de déceler à terme les opérations d'influences étrangères, est en cours de discussion et fera l'objet d'une première stabilisation au mois de septembre 2024* ».

Aussi, le très faible nombre de signalement effectués par le ministère résulte selon toutes vraisemblances des limites de son dispositif de détection. Dans ses réponses au questionnaire du rapporteur, le HFDS énonce clairement que « *les établissements font état d'une perception de la menace, mais ne parviennent qu'exceptionnellement, faute d'une grille de lecture opérationnelle, à caractériser des incidents dans les faits* ».

Lors de son audition, le HFDS a ainsi indiqué que seuls deux signalements ont été effectués au titre d'opérations d'ingérence en 2023 : « *nous avons eu deux cas l'an passé où nous avons caractérisé l'infraction d'ingérence, le premier a déclenché un signalement au procureur ; le deuxième était issu de nos investigations, parce que nous trouvions suspectes les réponses apportées par l'établissement aux questions que nous lui posions, c'est notre questionnement qui nous a conduits à identifier cette ingérence - une procédure disciplinaire est en cours dans ce dossier* »¹.

En sus, la commission d'enquête relève que **le dispositif ne couvre pas, ni même n'associe, les établissements d'enseignement supérieur et de recherche privés**, qui peuvent pourtant également constituer une cible stratégique pour des opérations d'influence malveillantes.

c) Des présidents d'universités volontaires mais souvent insuffisamment soutenus

(1) Une prise de conscience inégale ?

Compte tenu du principe d'autonomie des universités, **les chefs d'établissements sont appelés à jouer un rôle essentiel dans la mise en œuvre d'actions de prévention des opérations d'influences étrangères malveillantes**.

À ce sujet, Benjamin Leperchey, directeur adjoint à la DGESIP, a indiqué lors de son audition que la prise de conscience de ces enjeux était inégale selon les chefs d'établissements : « *Il n'y a pas de naïveté sur le sujet, mais la prise de conscience reste hétérogène parmi les présidents d'établissement. (...) Les établissements qui sont le plus au cœur de ces problématiques, comme l'Inalco, sont parfaitement au fait de l'ampleur de la menace et sont bien outillés pour adapter le contenu de leurs enseignements, leur posture et leurs partenariats en fonction du risque d'ingérence. Ils travaillent avec des ministères régaliens particulièrement prescripteurs. Dans les établissements sensibles, le sujet est parfaitement sous contrôle. Dans les établissements plus généralistes, nous pourrions craindre des ingérences moins visibles, plus évanescantes. La prise de conscience est réelle, mais*

¹ [Audition](#) du 14 mai 2024.

un recensement exhaustif est plus difficile à réaliser que dans le champ des sciences dures »¹.

Cette déclaration a suscité une grande incompréhension de la part de France Universités, l'association qui représente les chefs d'établissement auprès des pouvoirs publics. Son président a assuré le rapporteur, lors de son audition², de la mobilisation totale des chefs d'établissements, qui pâtissent plutôt d'un manque d'accompagnement de la part du ministère.

(2) Un manque de formation

En premier lieu, France université pointe une **formation insuffisante à ces enjeux des chefs d'établissements, et, au-delà, de la communauté académique dans son ensemble (chercheurs, associations étudiantes...)**.

Ce constat n'est pas démenti par le HFDS du ministère, qui, lors de son audition, indiquait clairement que : « *Depuis quelques années, l'essentiel du travail de formation porte sur les questions de laïcité et de séparatisme, notamment les valeurs de la République. Nous n'avons pas vraiment de formation spécifique sur les ingérences étrangères, hormis une à l'Institut des hautes études de l'éducation et de la formation. Pour autant, il y a des spécialistes de ces sujets dans le monde universitaire* »³.

(3) Un manque de moyens

France universités a également déploré leur manque de moyens pour mettre pleinement en œuvre la politique de prévention des ingérences dans les universités.

Ils déplorent l'absence de ligne budgétaire pour les accompagner dans la mise en place des ZRR, qui supposent la mobilisation de moyens conséquents par les universités : surveillance des systèmes d'information, utilisation d'appareils protégés, contrôle des entrées et des sorties...

Lors de son audition, la Ministre a entendu nuancer ce constat, en déclarant que le ministère accompagnait les bien les chefs d'établissements qui seraient placés en difficulté, sans toutefois fournir davantage de précisions sur la nature de cet accompagnement : « *oui, les ZRR représentent un surcoût. Le président d'université est le seul qui peut décider de placer un laboratoire ou une partie de laboratoire sous ce statut, mais nous l'accompagnons. J'aimerais avoir la liste des ZRR dont la mise en place serait aujourd'hui impossible pour des raisons de coût. De tels problèmes durent rarement plus d'un semestre, le temps d'élaborer un plan de financement. Nous accompagnons les universités dans ces problématiques, même s'il y a parfois des délais ; je ne crois pas qu'il y ait de réels blocages* »⁴.

¹ [Audition](#) du 2 mai 2024.

² [Audition du rapporteur](#), 3 juin 2024.

³ [Audition](#) du 14 mai 2024.

⁴ [Audition](#) du 18 juin 2024.

La longueur et la complexité des procédures est également mise en cause, de telle sorte qu'environ **150 à 200 ZRR seraient aujourd'hui en attente**, ordre de grandeur confirmé par la Ministre au cours de la même audition.

(4) Un défaut de pilotage

Lors de leur audition par le rapporteur, le président de France universités et le président de l'Inalco ont regretté **l'absence de directives claires de la part du ministère en matière de prévention des influences étrangères**.

En particulier, les représentants de l'Inalco ont indiqué que, face à ces risques, le principal problème n'était pas celui de la « *naïveté des chercheurs* », dans l'ensemble bien au fait de ces menaces, que de « *l'absence de processus balisé pour les aider à savoir comment y faire face* »¹.

C'est la raison pour laquelle **l'Inalco**, qui est particulièrement exposé aux risques d'influences étrangères, a commencé très récemment, **depuis la fin de l'année 2023, à mettre en place son propre dispositif de détection**, en formalisant, en lien avec son fonctionnaire de sécurité et de défense (FSD), des « *procédures de due diligence (vérifications nécessaires) et de reporting (signalement) pour centraliser les points d'alerte* » en matière d'ingérences. L'établissement entend aussi produire un « *manuel de bonnes pratiques* » à destination de sa communauté.

Si cette initiative ne peut qu'être louée et encouragée, son caractère extrêmement récent indique un certain retard dans la prise de conscience de la menace par le monde académique. Surtout, le fait que ce plan ait dû être conçu de façon autonome par l'université, sans aucunes lignes directrices émises au niveau national, illustre bien l'absence de pilotage de cette politique.

La commission d'enquête ne peut que regretter le fait que la conception de tels dispositifs de détection et de prévention repose sur les seules initiatives des chefs d'établissements, certes en lien avec leurs FSD, alors même qu'ils ne disposent pas nécessairement de la formation adéquate pour le faire. **Une initiative nationale, piloté par le HFDS et politiquement portée au niveau du ministre, permettant une généralisation de tels dispositifs serait nécessaire. Dans le respect du principe d'autonomie des universités, toute latitude serait ensuite laissée aux chefs d'établissements pour leur mise en œuvre opérationnelle.**

¹ *Audition du rapporteur, 3 juin 2024.*

3. Un dispositif qui reste marqué par d'importantes lacunes, et en particulier par un défaut d'application des recommandations les plus substantielles du « rapport Gattolin »

a) Une mise en œuvre parcellaire des recommandations du « rapport Gattolin »

Les travaux de la commission d'enquête ont mis en évidence une mise en œuvre parcellaire des recommandations du « rapport Gattolin » précité fait au nom de la mission d'information du Sénat sur les influences étrangères dans le monde universitaire et académique, trois ans après son adoption.

À sa demande, le HFDS a produit un état des lieux détaillé de leur mise en œuvre à date, qui figure en annexe du présent rapport. Le tableau et les éléments ci-après en synthétisent le contenu.

DOCUMENT PROVISOIRE

État d'application des recommandations de la mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences (2021) présenté par le ministère de l'Enseignement supérieur et de la Recherche

	Recommandation	État d'application selon le ministère
1	Dresser un état des lieux des alertes, de la volumétrie des signalements et des mesures prises pour y remédier et évaluer le niveau des influences étrangères dans l'enseignement supérieur et la recherche	Action en cours
2	Constituer un comité scientifique, prenant la forme d'un « observatoire des influences étrangères et de leurs incidences sur l'enseignement supérieur et la recherche » qui associerait universitaires, ministères de l'enseignement supérieur et de la recherche, des affaires étrangères, de l'économie, de l'intérieur et des armées, chargé de dresser un état des lieux, d'en assurer le suivi régulier et de formuler des propositions au Gouvernement	Action non engagée
3	Charger le comité d'élaborer une étude scientifique de référence sur l'état des menaces constatées en France. Ce document, qui ferait l'objet d'un suivi actualisé et d'une analyse des évolutions dynamiques, comporterait une vision globale des menaces extra-européennes et une cartographie des risques à la fois thématiques et géographiques	Action non engagée
4	Prévoir la transmission de cette étude et de ses versions actualisées au Parlement. Ses constats pourront faire l'objet d'un débat	Sans objet
5	Étendre le dispositif de protection du PPST à l'ensemble des disciplines universitaires, notamment en les adaptant aux enjeux et influences spécifiques aux sciences humaines et sociales qui en sont exclues	Action en cours
6	Confier au collège de déontologie de l'enseignement supérieur, de la recherche et de l'innovation une mission renforcée d'animation du réseau des déontologues au sein des établissements et à la procédure d'identification	Action menée

7	Assurer sur une base régulière un échange d'informations entre le collège de déontologie et le HFDS du MESR, sur toute question relative aux influences étrangères menaçant les libertés académiques	Action non engagée
8	En lien avec le collège de déontologie, renforcer le service du HFDS et le doter d'une expertise dédiée	Action en partie engagée
9	Constituer un réseau formalisé des fonctionnaires de sécurité et de défense (FSD), afin de leur permettre de bénéficier de l'expertise des services des ministères, d'échanger sur leurs pratiques et de centraliser les signalements	Action menée
10	Confier aux FSD, dont l'autorité et l'expertise seraient réaffirmées, et en lien avec le déontologue, un rôle de formation et de sensibilisation de l'ensemble de la communauté académique sur les risques liés aux influences extra-européennes. Cette action serait renforcée dans les domaines ou les zones identifiées comme potentiellement les plus à risque par le document de référence	Action menée
11	Élaborer et diffuser auprès des établissements via le réseau des FSD un guide de bonnes pratiques de coopération avec certains pays identifiés, guide qui doit être largement diffusé auprès de toute la communauté académique	Action en cours
12	Assurer une sensibilisation des collectivités territoriales, notamment régions et les grandes métropoles sur ces sujets, compte tenu de leur place significative dans les conseils d'administration des établissements d'enseignement supérieur	Action en cours
13	Étendre le bénéfice de la protection fonctionnelle à l'ensemble de la communauté académique (chercheurs non agents publics, institutions)	Action en cours
14	Généraliser la réalisation par l'Anssi d'un audit sur la sécurité des systèmes informatiques des universités, en y intégrant la question de la confidentialité des cours en ligne	Action non engagée
15	Renforcer les moyens dédiés à la détection et à la protection du monde universitaire et académique face aux interférences extérieures en inscrivant des crédits dédiés dans les budgets des universités et du ministère de l'Europe et des affaires étrangères	Action en cours

16	Prévoir, dans le cadre des décrets qui doivent être publiés au titre de l'article L. 211-2 du code de l'éducation, et en s'inspirant de l'article L. 411-5 du code de la recherche, l'obligation pour les chercheurs de signaler dans leurs thèses, travaux post doctoraux et publications scientifiques les éventuelles aides directes et indirectes dont ils ont pu bénéficier de la part d'États extra-européens	Action en partie engagée
17	Créer un régime de transparence sur l'origine des financements extra-européens des projets (colloques, contrats doctoraux, chaires...) menés par les établissements d'enseignement supérieur et de recherche et les <i>think-tanks</i>	Action non engagée
18	Faire valoir au niveau national des exigences de réciprocité dans les échanges universitaires avec les pays extra européens.	Action menée
19	Inclure systématiquement une clause relative au respect des libertés académiques et de l'intégrité scientifique dans les conventions passées avec les institutions et entreprises extra-européennes	Action non engagée
20	Modifier l'article L. 123-7-1 et l'article D. 123-19 du code de l'éducation pour prévoir une saisine pour avis des ministères concernés (enseignement supérieur et recherche, économie, affaires étrangères, intérieur et armées s'il y a lieu) sur les projets d'accord	Action en partie engagée
21	Modifier les mêmes articles pour fixer à trois mois maximum le délai d'examen des projets d'accord, pour permettre des investigations sérieuses	Action non engagée
22	Prévoir que les accords de recherche passés avec les filiales françaises des entreprises étrangères extra-européennes soient soumis systématiquement à la procédure d'examen	Action non engagée
23	Au niveau national, étudier l'adoption d'un corpus de moyens juridiques, d'ordre administratif et le cas échéant pénal, visant à sanctionner les interférences portant atteintes aux libertés académiques et à l'intégrité scientifique	Action en cours

24	Au niveau européen, mettre à profit la Présidence française de l'Union européenne pour proposer une stratégie ambitieuse de diplomatie scientifique, à la fois défensive, mais également offensive, dans la lignée du début de prise de conscience de nos partenaires	Action menée
25	Inciter au niveau européen et international à la création d'un classement des universités fondé sur le respect des libertés académiques et de l'intégrité scientifique, afin de mettre en lumière nos valeurs, par opposition à un classement de Shanghai devenu trop prescripteur	Absence d'observation
26	Promouvoir une norme européenne et internationale de clarification des échanges universitaires fondée sur le devoir de diligence (due diligence) et la conformité (compliance) à des lignes directrices fondées sur le respect de la liberté académique et l'intégrité scientifique, en accord avec la déclaration de Bonn du 23 octobre 2020 et les travaux de l'OCDE	Action menée

Source : commission d'enquête, d'après les réponses au questionnaire du rapporteur adressé au Haut fonctionnaire de défense et de sécurité du ministère de l'Enseignement supérieur et de la recherche

(1) Certaines actions ont bien été menées mais doivent désormais trouver une traduction concrète

Cet état des lieux permet, tout d'abord, de constater que **des actions ont bien menées pour appliquer certaines recommandations du rapport (6 sur 26)**, même s'il conviendra de veiller à ce que celles-ci se traduisent concrètement dans les faits.

Il s'agit notamment des recommandations tendant à :

- constituer un réseau formalisé des fonctionnaires de sécurité et de défense (FSD) afin de leur permettre de bénéficier de l'expertise des services des ministères, d'échanger sur leurs pratiques et de centraliser les signalements, même s'il a été montré *supra* que ce réseau doit encore être fortement renforcé eu égard aux besoins ;

- confier aux FSD, dont l'autorité et l'expertise seraient réaffirmées, et en lien avec le déontologue, un rôle de formation et de sensibilisation de l'ensemble de la communauté académique sur les risques liés aux influences extra-européennes, ce rôle étant conforté par une circulaire SDS / n° 2023-2212 du 25 mai 2023, communiquée à la commission d'enquête. L'enjeu sera ici de mettre en application ce rôle de formation dans les faits, et surtout de prendre en compte dans ce cadre la problématique des influences étrangères ;

(2) Certaines actions ont en partie été engagées

Le bilan du HFDS indique que des actions sont « en partie été engagées » sur certaines recommandations (3 sur 23). **La commission d'enquête relève cependant que l'engagement de ces actions est dans deux cas extrêmement récent, alors même que le rapport Gattolin a été publié il y a trois ans.**

Il s'agit notamment des recommandations tendant à :

- renforcer le SDS et le doter d'une expertise dédiée : comme cela a été montré *supra*, les effectifs du SDS ont bien connu une montée en puissance, appelée à se poursuivre. En revanche, celui-ci n'intègre à ce stade pas d'expertise dédiée à la problématique des influences étrangères ;

- instaurer un régime de transparence sur les financements et les liens d'intérêts extra-européens des chercheurs : le HFDS a indiqué à cet égard qu'un groupe de travail, piloté par le SGDSN avait été constitué et travaille à pouvoir instaurer, de manière effective, une exigence la déclaration par les candidats de leurs éventuels conflits d'intérêts dans les demandes d'accès aux zones à régime restrictif. Cette initiative est certes louable, mais encore insuffisante compte tenu de son périmètre limité aux ZRR, à plus forte raison compte tenu du fait que celles-ci ne concernent généralement pas les sciences humaines et sociales, qui sont pourtant une cible de premier plan des opérations d'influences étrangères (*voir supra*) ;

- prévoir une saisine pour avis des ministères concernés sur les projets d'accord : à nouveau, il est indiqué qu'un groupe de travail piloté par le SGDSN, dont la première réunion s'est tenue le 25 avril 2024, et auquel participent tous les ministères concernés par la réglementation relative à la PPST, travaille à pouvoir instaurer, par voie réglementaire, une obligation de saisine pour avis sur les projets de coopération internationale en cas d'implication d'une unité de recherche protégée par la PPST. Le non-respect de cette obligation donnerait lieu à une contravention.

(3) Certaines actions sont en cours, et doivent être menées à leur terme

Certaines recommandations (7) ont donné lieu à des actions qui sont en cours, et qu'il convient désormais de mener à leur terme.

Il s'agit notamment des recommandations tendant à :

- dresser un état des lieux des alertes, même s'il a été montré *supra* que le dispositif actuel de détection n'était pas à la hauteur des enjeux ;

- étendre le dispositif de PPST à l'ensemble des disciplines universitaires : à cet égard, il a été indiqué que, dans le sillage de la réforme des PPST, un arrêté interministériel était en cours d'élaboration, et devrait étendre le champ des PPST à de nouveaux domaines (sciences cognitives et neurosciences, sciences du langage, psychologie notamment). Si cette évolution va dans le bon sens, elle est cependant insuffisante puisque

l'ensemble des sciences humaines et sociales sont susceptibles de faire l'objet d'opérations d'influences étrangères ;

- élaborer et diffuser auprès des établissements via le réseau des FSD un guide de bonnes pratiques de coopération avec certains pays identifiés : là encore : à nouveau, il est indiqué qu'un groupe de travail piloté par le SGDSN, dont la première réunion s'est tenue le 25 avril 2024 et auquel participent tous les ministères concernés par la réglementation relative à la PPST, travaille à fournir aux entités intéressées, notamment aux établissements d'ESR, un guide et une grille d'auto-évaluation préliminaire des projets de coopération. Le ministère précise qu'il appartient au seul SGDSN, le cas échéant, de mettre à la disposition des établissements des documents relatifs à des États en particulier ;

- assurer une sensibilisation des collectivités territoriales : le ministère indique qu'un plan de sensibilisation a bien été engagé en juillet 2022, mais en précisant que celui-ci se concentre sur les enjeux d'intelligence économique, et ne concerne donc qu'à la marge la thématique des influences étrangères.

- étudier l'adoption d'un corpus de moyens juridiques, d'ordre administratif et le cas échéant pénal, visant à sanctionner les interférences portant atteintes aux libertés académiques et à l'intégrité scientifique : le ministère cite à cet égard la réforme du dispositif de PPST, détaillée *supra*.

(4) Sur les 26 recommandations, 8 n'ont donné lieu à aucune action à ce jour

Enfin, le document transmis par le ministère indique que **8 recommandations sur 26 n'ont donné lieu à aucune action, ce que la commission d'enquête ne peut que regretter.**

Il s'agit principalement des recommandations tendant à :

- créer un **observatoire des influences étrangères et de leurs incidences sur l'enseignement supérieur et la recherche** : à cet égard, le ministère indique que « *la diversité et la porosité des moyens et des cibles des opérations d'influence étrangère ne rendent pas pertinente une segmentation de l'action interministérielle sur ces problématiques, qu'il est nécessaire d'envisager dans leur ensemble et leur complexité* ». La commission d'enquête souscrit à cette analyse, considérant que la lutte contre les influences étrangères malveillantes requiert une approche globale, s'inscrivant dans le cadre d'une stratégie interministérielle. Tout en restant convaincu de la nécessité de se doter d'instances permettant d'améliorer notre connaissance fondamentale du phénomène, il formulera ainsi *infra* une recommandation tendant à la création d'un observatoire au périmètre élargi (voir *Troisième partie, I*).

- créer un régime de transparence sur l'origine des financements extra-européens dont bénéficient établissements d'enseignement supérieur et de recherche privés : recommandation que le ministère juge pertinente dans son principe, mais qui requiert une modification de la loi ;

- prévoir que les accords de recherche passés avec les filiales françaises des entreprises étrangères extra-européennes soient soumis systématiquement à la procédure d'examen des projets d'accord par le ministère : recommandation que le ministère juge pertinente dans son principe, mais qui requiert une modification de la loi.

b) Un nouveau point de fragilité identifié : les bourses à financement étatique ou para-étatique

Les travaux de la commission d'enquête ont permis de mettre en évidence un nouveau point de fragilité des universités vis-à-vis des opérations d'influences étrangères : le contrôle insuffisant des bourses octroyées par des États ou structures para-étatiques.

Lors de son audition, la ministre Sylvie Retailleau a ainsi indiqué que : « *une vigilance renforcée est portée sur certaines associations, notamment celles d'étudiants étrangers, qui ont souvent des liens avec les gouvernements de leurs pays respectifs. Nous nous intéressons à certaines bourses à financement étatique, particulièrement celles du China Scholarship Council (CSC), dont il est documenté que les bénéficiaires doivent rendre compte à l'ambassade de Chine ou à ses proxys* ».

La commission d'enquête ne peut que partager cette préoccupation. Si la présence en France de chercheurs et d'étudiants étrangers est une richesse indispensable à l'écosystème académique national tant en termes de ressources humaines que financières, les bourses à financement étatique ou para-étatique – ainsi celles proposées par le *China Shcolarship Council* – doivent probablement être mieux et systématiquement encadrées pour limiter les risques, identifiés par le HFDS du ministère dans ses réponses au questionnaire du rapporteur, liés à « *l'exposition des intérêts fondamentaux de la Nation aux servitudes des boursiers vis- à-vis de leurs financeurs* ».

D. LE CHAMP ÉCONOMIQUE ET INDUSTRIEL : UN ARSENAL LÉGISLATIF RELATIVEMENT COMPLET, MAIS UNE PRISE EN COMPTE ENCORE INSUFFISANTE DES ENJEUX DE SÉCURITÉ INFORMATIONNELLE

La commission d'enquête s'est également intéressée, au cours de ses travaux, à la thématique de la sécurité économique.

Celle-ci ne recoupe qu'en partie le périmètre de la commission d'enquête dans la mesure où, comme cela a été rappelé en introduction du présent rapport, la **sécurité économique, et l'enjeu de protection de nos actifs, technologies et données stratégiques, qui sont des attributs de puissance « dure », ne relève en général pas de la guerre d'influence.**

Cependant, les opérations d'influence constituent cependant bien l'un des trois piliers de l'intelligence économique. De telles opérations « *visent à convaincre, séduire ou dissuader les organismes décideurs évoluant dans*

l'environnement direct d'une entreprise »¹. En particulier, l'atteinte réputationnelle qui pourrait être portée à des entreprises françaises dans le cadre de manipulations de l'information peuvent relever à la fois de la guerre économique et de la guerre d'influence menées, simultanément contre les entreprises concernées pour des raisons économique et contre la France pour des raisons politiques.

1. L'action du Sisse, « bras armé du Gouvernement » en matière de sécurité économique

a) *Une mission de veille et d'alerte sur les menaces économiques qui monte en puissance, mais un maillage territorial encore insuffisant*

Le bras armé de la politique de sécurité économique du Gouvernement est le Service de l'information et de la sécurité économiques (Sisse), lequel est un service de la Direction générale des entreprises (DGE). Il possède en outre une compétence interministérielle, avec un rôle de coordination de toutes les administrations concourant à cette politique. La mission essentielle de ce service est de protéger les actifs stratégiques de l'économie française, matériels et immatériels, face aux menaces étrangères.

Le Sisse travaille sur la base de trois listes structurantes d'actifs stratégiques, qui correspondent aux entités sur lesquelles il veille. Elles concernent respectivement :

- les d'entreprises stratégiques qui répond, selon le chef du Sisse auditionné par la commission d'enquête, Joffrey Célestin-Urbain, à une « *approche large de la sécurité économique* », en ce que celle-ci « *va bien au-delà du CAC 40 et du SBF 120 et bien au-delà des seules entreprises de la défense et de la sécurité* »² ;

- une liste de technologies critiques pour l'économie française, qui représente une vision prospective du potentiel d'innovation que nous voulons protéger ;

- une liste plus récente des laboratoires publics de recherche sensible, élaborée en lien avec le ministère de l'enseignement supérieur, de la recherche.

Le nombre d'entreprises appartenant à ces listes est confidentielle et ne peut être diffusée dans le cadre du présent rapport. En particulier, parce qu'une entreprise n'est pas informée de son inscription.

Son travail consiste à collecter et traiter toute information potentiellement pertinente qui révélerait une menace étrangère sur l'une de ces entreprises, technologies ou laboratoires : son chef décrit ainsi le Sisse

¹ [Rapport d'information n° 872 \(2022-2023\)](#) fait par Marie-Noëlle Lienemann et Jean-Baptiste Lemoyne au nom de la commission des affaires économiques du Sénat sur l'intelligence économique, déposé le 12 juillet 2023.

² [Audition](#) du 9 avril 2024.

comme « une machine à aspirer des informations en provenance des services de l'État, les services de renseignement étant notre source la plus importante, mais aussi de nos propres capacités de veille, qui nous permettent de repérer dans nos bases de données des faisceaux d'indices, des menaces futures, des signaux faibles ».

À cette fin, le Sisse a mis en place en 2020 une plateforme de veille interministérielle en 2020, recensant les menaces économiques étrangères. Celles-ci sont passées de 353 en 2020 à 478 en 2021, 694 en 2022, 968 en 2023. Pour le chef du Sisse, cette augmentation s'explique par deux types de facteurs : une montée brute de la menace étrangère, liée à des raisons structurelles relevant de la géopolitique mondiale, et la montée en puissance du dispositif lui-même.

Les deux principales catégories de menaces identifiées dans ce cadre sont constituées par :

- un risque de prise d'influence par voie capitalistique par un acteur étranger dans près de la moitié des cas en 2023 ;
- un risque de captation de données sensibles ou de propriété intellectuelle dans environ 40% des cas.

Le Sisse a indiqué au rapporteur qu'il restait par ailleurs vigilant à l'émergence de nouvelles formes de menaces, en lien notamment avec l'intensification de l'utilisation de l'arme normative et usages stratégiques du droit (*lawfare*), l'activisme ou les ruptures volontaires d'approvisionnement.

Pour mener à bien ces missions, le Sisse emploie au total 58 ETP, dont :

- 34 agents en administration centrale, organisés autour d'une chaîne de veille et de traitement des menaces économiques ;
- 24 agents en réseau déconcentré : les délégués à l'information stratégique et à la sécurité économique (Disse) placés sous l'autorité conjointe du Préfet de région et du directeur de la Direction régionale de l'économie, de l'emploi, du travail et des solidarités (Dreets) au sein de laquelle ils sont positionnés, ont plusieurs missions, notamment, de conseiller les entreprises face aux risques de sécurité économique, et d'effectuer une veille stratégique, se traduisant par des remontées d'informations de terrain à la demande du Sisse ou à son initiative sur les menaces étrangères et les vulnérabilités des entreprises stratégiques dans leur ressort régional.

Lors de son audition, le chef du Sisse a néanmoins fait état d'une certaine insuffisance de moyens de ce réseau déconcentré : « concernant l'identification des Disse par les entreprises, nous nous sommes, faute de ressources adaptées à un changement d'échelle, arrêtés à mi-chemin. Avec seulement vingt délégués en région, il est impossible de sillonnner le terrain ».

b) Un arsenal législatif jugé complet

Face aux menaces pour la sécurité économique, plusieurs instruments interministériels peuvent être mobilisés, qui vont de l'action informelle à la

mise en jeu de la « loi de blocage » du 26 juillet 1968¹ pour protéger les entreprises françaises d'une application extraterritoriale d'un droit étranger ou encore le recours, mentionné *supra*, au dispositif de protection du potentiel scientifique et technique de la Nation (voir *encadré*).

DOCUMENT PROVISOIRE

¹ Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.

Les instruments interministériels concourant à la sécurité économique

Cinq catégories d'instruments sont répertoriées par le Service de l'information et de la sécurité économiques (Sisse) :

1° Les actions informelles : la mise en place d'un dispositif opérationnel de sécurité économique permet d'orienter les capteurs et d'anticiper les menaces pesant sur les actifs stratégiques pour l'économie française. Ainsi, les services de l'État peuvent tenter d'éviter ou atténuer la menace avant qu'elle ne se matérialise et nécessite une remédiation formelle, financière ou juridique, qui implique des contraintes d'exécution. Aussi, une partie importante de l'activité de remédiation pilotée par le Sisse relève d'actions informelles, en lien avec les entreprises visées, voire leurs actionnaires. L'interministériel mène notamment des actions de sensibilisation (en particulier des services de renseignement ou des services déconcentrés), des propositions d'accompagnement, des échanges avec les entreprises, etc.

2° Le contrôle des investissements étrangers en France (IEF), dont le pilotage est assuré par la Direction générale du Trésor, dans le cadre du comité interministériel des investissements étrangers en France (CIIEF). Les évolutions successives du dispositif IEF en 2020 et 2023 ont permis le renforcement de la protection des entreprises stratégiques face aux menaces économiques étrangères. En outre, un dispositif interministériel de suivi des conditions imposées aux investisseurs au titre du contrôle des IEF est désormais déployé sous la coordination du Sisse et de ses délégués en région (Disse). La mise en place de ce dispositif de suivi garantit la crédibilité du mécanisme de contrôle des IEF. Il s'inscrit dans un objectif général de contrôler une centaine de lettres par an, en mobilisant l'ensemble des ministères compétents.

3° La loi du 26 juillet 1968 dite « loi de blocage », qui constitue l'un des principaux outils français de protection des entreprises face à l'application extraterritoriale de normes étrangères. Son article 1^{er} interdit la communication à toute autorité publique étrangère d'informations touchant nos intérêts économiques essentiels. Son article 1^{er bis} interdit toute transmission d'information susceptible de servir de preuve dans le cadre d'une procédure administrative ou judiciaire, indépendamment de la sensibilité de l'information. La loi de 1968 a été redynamisée par décret le 18 février 2022¹, avec la création d'un guichet unique d'accompagnement des entreprises, assuré par le Sisse, qui émet désormais des avis de conformité. Le guichet est rapidement monté en charge (98 saisines en deux ans contre moins de 10 par an avant 2020).

4° Les leviers financiers, avec la mobilisation de certains fonds publics, en lien avec Bpifrance, et notamment la proche d'investissement *French Tech Souveraineté* (FTS).

5° Le dispositif de protection du potentiel scientifique et technologique de la Nation (PPST), qui vise à lutter contre la captation scientifique et technologique en empêchant de façon ciblée des individus/entités d'accéder aux savoirs et savoir-faire sensibles à la fois à des fins de contre-prolifération, de contre-terrorisme, mais aussi de sécurité économique. La PPST, dans sa forme actuelle, repose sur deux piliers principaux : (i) la création de zones protégées baptisées zones à régime restrictif (ZRR) au sein des établissements et (ii) le contrôle des coopérations internationales.

Source : réponses du Sisse au questionnaire du rapporteur

¹ Décret n° 2022-207 du 18 février 2022 relatif à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères

La décision de mobiliser l'un de ces instruments est, le cas échéant, prise dans le cadre du **Comité de liaison en matière de sécurité économique (Colise)**, qui est présidé par le SGDSN et dont le secrétariat est assuré par le Commissaire à l'information stratégique et à la sécurité économique (CISSE). Il comprend, en outre, le Coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT) ainsi que les représentants des ministres chargés de l'économie et des finances, de l'intérieur, des affaires étrangères, de la transition écologique, des armées, du travail de la santé, de l'enseignement supérieur et de la recherche, et de l'agriculture.

Cet éventail de réponses est jugé complet par le chef du Sisse, qui a déclaré, dans son audition, ne pas voir « *d'angle mort majeur* », considérant par ailleurs que « *la voie réglementaire permet de pallier les manques* », comme l'a illustré la redynamisation de la « loi de blocage » de 1968 par le décret du 18 février 2022 (voir encadré). Dans ses réponses au questionnaire du rapporteur, le Sisse indique explicitement, à court terme, il « *n'identifie pas de besoin d'évolution législative ou réglementaire majeur. Le dispositif interministériel de sécurité économique piloté par le Sisse est monté en puissance depuis sa refonte en 2019 et arrive en régime de croisière* ». *DOC INTEGRALE PROTEGEE*

À ce titre, on peut citer les rapports du sénateur Philippe Bonnecarrère du 4 octobre 2018 sur l'extraterritorialité des sanctions américaines¹ et du 6 avril 2018 sur la protection des savoir-faire et des informations commerciales non divulgués contre l'obtention, l'utilisation et la divulgation illicites².

2. Les opérations d'influence étrangère : un « angle mort » de la politique de sécurité économique

La commission d'enquête tient cependant à souligner que l'approche actuelle retenue de la politique de sécurité économique laisse vacante la question des opérations d'influence étrangères qui pourraient cibler l'économie française dans un but politique.

Deux cas méritent à cet égard d'être considérés.

En premier lieu, il convient d'envisager le cas où des investissements réalisés dans un but politique d'influence et de « puissance douce » seraient réalisés, mais pourraient potentiellement préparer le

¹ [Rapport d'information n° 17 \(2018-2019\)](#) fait par Philippe Bonnecarrère au nom de la commission des affaires européennes du Sénat sur l'extraterritorialité des sanctions américaines, déposé le 4 octobre 2018.

² [Rapport d'information n° 406 \(2017-2018\)](#) fait par Philippe Bonnecarrère au nom de la commission des affaires européennes du Sénat portant observations sur la proposition de loi transposant la directive du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulguées contre l'obtention, l'utilisation et la divulgation illicites, déposé le 6 avril 2018.

terrain à une politique d'influence plus agressive, voire à des opérations d'ingérences économiques.

À cet égard, le chef du Sisse a été interrogé, tant par la présente commission d'enquête que lors de son audition par la commission d'enquête de l'Assemblée nationale relative aux ingérences étrangères.

Devant cette dernière, il a ainsi pu déclarer qu'a priori, ce type d'opérations sans lien avec la sécurité économique stricto sensu en ce qu'elles ne portent pas sur des actifs stratégiques, méritent bien une certaine vigilance :

« Vous m'avez interrogé en particulier sur les stratégies de quatre États : la Chine, le Qatar, les Émirats arabes unis et l'Inde. Si la Chine est évidemment assez représentée dans les menaces que nous percevons, les trois autres pays le sont beaucoup moins. Les États qui nous intéressent sont ceux qui mènent une véritable stratégie de puissance et dont les investissements tendent à se concentrer assez systématiquement sur les filières stratégiques de notre pays. Les sujets immobiliers nous paraissent un peu moins stratégiques – il faut bien faire des choix ! Le Qatar et les Émirats arabes unis mènent une stratégie un peu différente : ils exercent un soft power, investissent dans le sport, mais nous n'avons pas repéré d'activité dans les secteurs stratégiques qui nous intéressent. Il en va de même pour l'Inde, qui ne représente pas pour nous une menace très significative en matière de sécurité économique. Mais le décollage économique de ce pays, notamment dans les filières très technologiques, est encore largement devant nous ; il n'est donc pas impossible que la situation vienne à changer. »

Notre système de détection étant totalement adaptable, si nous repérons une tendance ou identifions un pays qui commence à se manifester régulièrement dans nos écosystèmes stratégiques, nous pourrons réorienter nos capteurs et inciter la direction générale de la sécurité intérieure (DGSI), la direction générale de la sécurité extérieure (DGSE) et la direction du renseignement et de la sécurité de la défense (DRSD) à le surveiller de près »¹.

Certes, suivi de ce type d'opérations de puissance douce au niveau national par le Sisse ne paraît pas totalement en ligne avec le format actuel de ce service, comme l'a indiqué le chef du Sisse devant la commission d'enquête : « Le calibrage de notre dispositif est essentiel : nous sommes aujourd'hui capables de suivre les acteurs inscrits sur nos listes ; l'approche ne serait pas du tout la même si ce nombre croissait substantiellement »².

La commission d'enquête préconisera toutefois de faire évoluer en ce sens les missions du Sisse, en prévoyant la mobilisation des « capteurs » locaux que sont les Disse pour mieux détecter ce type d'opérations, sans

¹ [Rapport n° 1311 \(seizième législature\)](#) fait par Constance Le Grip au nom de la commission d'enquête de l'Assemblée nationale relative aux ingérences politiques, économiques et financières de puissances étrangères – États, organisations, entreprises, groupes d'intérêts, personnes privées – visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français, déposé le 1^{er} juin 2023, Tome II.

² [Audition](#) du 9 avril 2024.

nécessairement se référer à une liste nationale comme dans le cadre du régime des actifs stratégiques (voir *Troisième partie, II*).

Deuxièmement, il convient de prendre en compte le cas où des opérations d'intelligence économique prenant la forme d'atteinte réputationnelle contre des entreprises françaises s'inscriraient dans un objectif politique visant à nuire à l'image de la France.

Comme l'a indiqué le chef du Sisse lors de son audition, l'influence *stricto sensu* n'entre aujourd'hui pas dans le périmètre des menaces suivies par son service, tout en considérant que la question mérite bien d'être soulevée : « *le paysage de la menace économique étrangère comprend à la fois des ingérences caractérisées - et parfois des opérations illégales et clandestines - et des opérations nettement plus « habituelles » en économie de marché : lobbying, influence. Faut-il qualifier de menace pour la sécurité économique française les actions de lobbying des grandes plateformes du numérique à Bruxelles ? On aurait tendance à dire oui, mais, lorsque des entreprises françaises font de même, on penche plutôt pour dire qu'un tel lobbying relève du jeu légitime* »¹.

Pour autant, le chef du Sisse a indiqué lors de la commission d'enquête être « *favorable à l'élargissement du périmètre d'action du SISSE, afin de lui permettre notamment d'agir davantage en matière d'intelligence économique* », dont l'influence constitue un pilier.

En tout état de cause, le travail de veille sur des campagnes numériques qui cibleraient des entreprises présentes sur le territoire national à la seule fin de nuire à l'image de la France, en ce qu'elles portent atteinte aux intérêts fondamentaux de la Nation, ne relèveraient pas du Sisse mais plutôt de Viginum. La prise en compte accrue de ces enjeux devrait conduire à confier à Viginum la mission de mener sur le terrain des actions de sensibilisation et de formation des entreprises françaises à ces enjeux. La commission d'enquête formulera une recommandation en ce sens (voir *Troisième partie, IV*).

E. LE CHAMP ASSOCIATIF ET CULTUEL : MALGRÉ DES PROGRÈS RÉALISÉS DANS LE CONTRÔLE DU FINANCEMENT ÉTRANGER DES CULTES AINSI QUE DES ÉCOLES PRIVÉES HORS CONTRAT, DES ZONES D'OMBRE SUBSISTENT

Le secteur associatif et cultuel est également exposé aux opérations d'influence étrangères, passant en particulier par le levier du financement.

¹ [Audition](#) du 9 avril 2024.

1. Un dispositif de contrôle récemment renforcé par la loi confortant le respect des principes de la République

a) *Le financement étranger des cultes*

Il en va en particulier du financement étranger des structures, dont le cadre juridique a connu dernièrement des évolutions notables avec la loi du 24 août 2021 confortant le respect des principes de la République (loi CRPR)¹.

S'agissant des associations fondées sous le régime de la loi de 1901, l'article 4-2 de la loi du 23 juillet 1987 sur le développement du mécénat² issu de la loi CRPR impose aux associations et fonds de dotation recevant plus de 153 000 euros de dons de tenir un état comptable séparé des avantages et ressources lorsqu'ils bénéficient, directement ou indirectement, de ressources en provenance de l'étranger. Le non-respect de cette obligation est passible d'une amende de 3 750 euros, dont le montant peut être porté au quart de la somme des avantages et ressources provenant de l'étranger non-inscrits à l'état séparé. Les fiducies ou personnes morales de droit français concourant à ces financements étrangers peuvent par ailleurs être soumis à une obligation de certification de leurs comptes

S'agissant des associations cultuelles fondées sous le régime de la loi de 1905 et des associations mixtes fondées sous le régime de la loi du 2 janvier 1907 concernant l'exercice public des cultes³ :

- l'article 19-3 de la loi du 9 décembre 1905 concernant la séparation des Églises et de l'État issu de la loi CRPR impose à ces associations de déclarer à l'autorité administrative les financements qu'elles perçoivent directement ou indirectement en provenance de l'étranger lorsque leur montant ou valorisation dépasse 15 300 euros. Le non-respect de cette obligation est également passible d'une amende de 3 750 euros, dont le montant peut être porté au quart de la somme sur laquelle a porté l'infraction ;

- le même article confère à l'autorité administrative un droit d'opposition lorsque « *les agissements de l'association bénéficiaire ou de l'un de ses dirigeants ou administrateurs établissent l'existence d'une menace réelle, actuelle et suffisamment grave affectant un intérêt fondamental de la société* » :

- l'article 75 de la loi CRPR soumet les associations cultuelles à une obligation de certification de leurs comptes lorsque le montant total des ressources et avantages provenant de l'étranger excède 50 000 euros ainsi qu'à une obligation de tenue d'un état comptable séparé desdites ressources.

¹ Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République.

² Loi n° 87-571 du 23 juillet 1987 sur le développement du mécénat

³ Il convient de noter que ce régime est également applicable dans les départements du Bas-Rhin, du Haut-Rhin et de la Moselle, les associations inscrites de droit local à objet cultuel - exclusif ou non - sur le fondement de l'article 79-VIII du code civil local.

Entre le 25 avril 2022, date d'entrée en vigueur du dispositif¹, et le 1^{er} juillet 2024, les services du ministère de l'Intérieur ont indiqué à la commission d'enquête que :

- 2 522 déclarations avaient été effectuées, au titre de 13 496 opérations de financement ;
- ces déclarations représentent un total de 108,6 millions d'euros.

Les financements déclarés concernent principalement les cultes protestants (40,6 %) et musulman (19,6 %).

DOCUMENT PROVISOIRE

¹ Suite à la publication du décret d'application n° 2022-619 du 22 avril 2022

**Financements étrangers déclarés entre le 25 avril 2022 et le 1^{er} juillet 2024 –
ventilation par culte**

(en millions d'euros et en pourcentage)

	Montant	Pourcentage
Protestants	44,1	40,6 %
Musulmans	21,3	19,6 %
Mormons	10,6	9,8 %
Témoins de Jéhovah	8,5	7,8 %
Catholiques	7,6	7,0 %
Autres (orthodoxes, Baha'ie, hindouistes, bouddhistes...)	16,5	15,2 %
Total	108,6	

Source : commission d'enquête, d'après les réponses de la direction des libertés publiques et des affaires juridiques au questionnaire du rapporteur

Les principaux pays d'origine de ces financements sont détaillés dans le tableau suivant. Comme le souligne la direction des libertés publiques et des affaires juridiques (DLPAJ) du ministère de l'intérieur dans ses réponses au questionnaire du rapporteur : « *la part de ces pays d'origine ne saurait s'expliquer par un unique facteur et tient à une pluralité de phénomènes, historiques, géographiques, culturels, migratoires...* ».

Interrogée sur ce point par le rapporteur, la DLPAJ a indiqué ne pas disposer de données à jour permettant de distinguer les États des autres personnes morales et physiques étrangères, ainsi que leur nationalité. Le rapporteur considère pourtant qu'une telle précision aurait son utilité, dans une logique de détections des opérations d'influences étrangères étatiques, tout en étant conscient qu'un acteur étatique qui s'engagerait dans ce type d'opération pourrait aisément passer par un intermédiaire.

Par ailleurs, la DLPAJ a indiqué au rapporteur que le droit d'opposition de l'administration à un financement étranger désormais prévu par la loi n'a pas encore trouvé à s'appliquer. Elle l'a cependant informé qu'une intention d'opposition a récemment été notifiée à une association.

La DLPAJ a en outre indiqué que, sur l'ensemble des déclarations effectuées :

- 235 ont fait l'objet d'une saisine des services de renseignement ;

- 28 courriers de demandes de pièces complémentaires ont été transmises à des associations.

S'agissant du non-respect de l'obligation de déclaration, il a été précisé, à date, que :

- les constats d'une absence de déclaration ou d'une déclaration incomplète ont donné lieu à deux transmissions au procureur de la République sur le fondement de l'article 40 du code de procédure pénale ;

- des investigations complémentaires sont en cours sur une vingtaine de dossiers afin de matérialiser un défaut de déclaration de financement étranger et donner lieu, le cas échéant, à une saisine du parquet compétent.

Financements étrangers déclarés entre le 25 avril 2022 et le 1^{er} juillet 2024 – ventilation par pays d'origine

(en millions d'euros et en pourcentage)

	Montant	Pourcentage
États-Unis	37,6	34,6
Allemagne	9,3	8,6
Suisse	9,2	8,5
Royaume-Uni	8,4	7,7
Algérie	8,0	7,4
Maroc	7,2	6,6
Turquie	5,4	5,0
Autres	23,5	21,6
Total	108,6	

Source : commission d'enquête, d'après les réponses de la direction des libertés publiques et des affaires juridiques au questionnaire du rapporteur

b) Une nouvelle obligation de déclaration d'intention d'aliéner les locaux culturels au profit de personnes étrangères

La loi CRPR a également prévu un dispositif de déclaration préalable à l'autorité administrative de toute aliénation d'un local servant habituellement à l'exercice public d'un culte consentie directement ou indirectement à un État étranger, à une personne morale étrangère ou à une personne physique non résidente en France¹.

En effet, comme l'avait alors relevé la commission des lois dans son rapport sur le texte lors de son examen au Sénat en première lecture en 2021 : « *De telles pratiques sont d'autant plus problématiques qu'elles présentent parfois l'avantage d'une solution rapide à des difficultés de financement de travaux ou de construction d'un lieu de culte. Dans le cas de la mosquée d'Angers, la difficulté à financer les travaux de construction de la mosquée ont ainsi été avancés comme argument par l'association ordonnant les travaux pour accepter la cession de la mosquée au royaume du Maroc, en échange d'un financement par celui-ci des travaux restant à effectuer. Pour ce qui concerne le culte musulman, il peut notamment être recouru à l'instrument du « waqf ». Les « waqf » ou « habous », sont généralement définis comme des fonds immobilisés, qui ne peuvent être ni donnés, ni vendus, et dont les revenus reviennent à l'organisation d'actions charitables, dont l'aumône »*².

c) Le contrôle des écoles privées hors contrat

Un second apport de la loi CRPR concerne les écoles privées hors contrat. En effet, ces doivent désormais répondre à de nouvelles obligations, de nature à permettre à l'administration de s'opposer à l'ouverture d'écoles hors contrat soutenues par un État étranger hostile à la République.

En premier lieu, l'article L. 441-1 du code de l'éducation relatif à l'obligation de déclaration préalable à l'ouverture d'une école privée hors contrat permet désormais au préfet de département de s'opposer à l'ouverture d'une telle école « *afin de prévenir toute forme d'ingérence étrangère ou de protéger les intérêts fondamentaux de la Nation* ».

L'article L. 441-3-1 du même code permet également au préfet, lorsqu'une association accueille des enfants aux fins de leur dispenser des enseignements scolaires sans que cette association ne se soit déclarée en tant qu'école privée hors contrat dans les conditions prévues à l'article L. 441-1 précité, de prononcer l'interruption de cet accueil et la fermeture des locaux utilisés.

L'article L. 441-4 du même code prévoit enfin que fait d'ouvrir un établissement d'enseignement scolaire privé en dépit d'une opposition formulée par les autorités compétentes ou sans remplir les conditions et

¹ Article 17-1 de la loi du 9 décembre 1905 concernant la séparation des Églises et de l'État.

² [Rapport n° 454 \(2020-2021\)](#) fait par Jacqueline Eustache-Brinio et Dominique Vérien au nom de la commission des lois du Sénat sur le projet de loi confortant les principes de la République, déposé le 18 mars 2021.

formalités prescrites constitue un délit puni d'un an d'emprisonnement et de 15 000 euros d'amende.

2. Un bilan globalement positif des nouveaux dispositifs issus de la loi confortant le respect des principes de la République, mais des lacunes et des zones d'ombres qui subsistent

a) Un bilan jugé globalement positif du nouveau régime de contrôle du financement étranger des cultes

Dans son rapport annuel d'activité au titre de l'année 2021¹, Tracfin avait alerté sur les risques liés au financements étrangers des associations.

Cette même année, le service a ainsi reçu plus de 700 signalements en lien avec des soupçons de financement du terrorisme ou de radicalisation impliquant des structures associatives. Près de la moitié concerne le financement d'associations cultuelles, dont l'objet déclaré est la gestion ou la construction de lieux de culte.

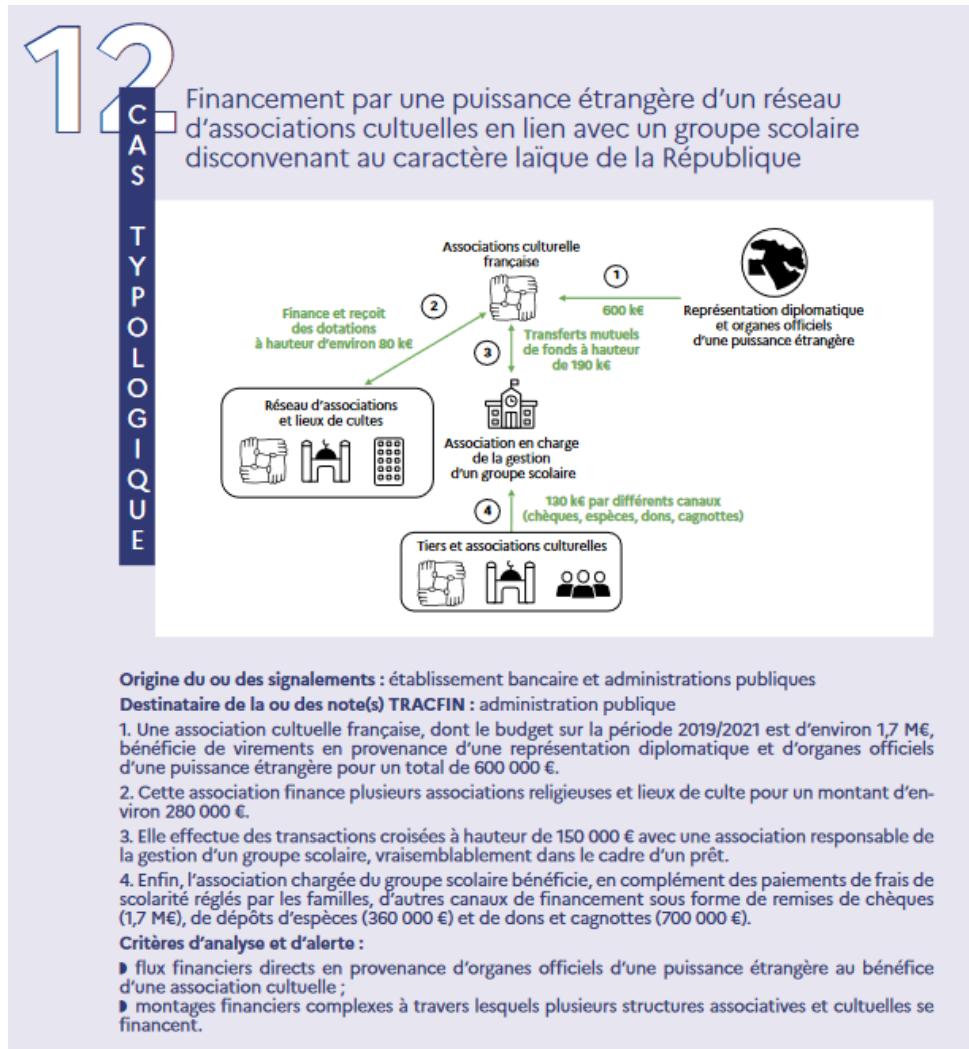
Les investigations qui avaient alors été réalisées mettaient en exergue « *une tendance à la dissimulation des fonds perçus par des réseaux associatifs cultuels. Celle-ci se matérialise soit par des montages financiers complexes faisant intervenir plusieurs structures associatives ayant des liens, sans justification économique apparente, avec des sociétés du secteur du bâtiment, soit par le non-respect des obligations de transparence comptable. Dans une moindre mesure, Tracfin a également constaté le recours à des collectes de fonds organisées sur des plateformes de cagnottes en ligne recueillant plusieurs centaines de milliers d'euros sans que l'identité des donateurs soit recueillie*

Comme le souligne le même rapport, les enquêtes relatives à ces financements étrangers opaques ont permis à Tracfin de caractériser des opérations d'ingérence : « *les circuits de financement observés par Tracfin confirment les risques d'ingérence de puissances étrangères par le biais de structures associatives promotrices d'une idéologie radicale. Ces dernières peuvent être financées directement au moyen de dotations et de virements provenant des organes officiels des États impliqués ou par de rebonds via des pays tiers*

À titre illustratif, Tracfin présente dans son rapport un schéma de cas typologique de montage complexe réalisé au titre du financement par une puissance étrangère d'un réseau d'associations cultuelles en lien avec un groupe scolaire disconvenant au caractère laïque de la République (voir ci-dessous).

¹ [Tracfin 2021, Activité et analyse](#), juillet 2022.

Cas-type de montage financier d'ingérence étrangère dans le domaine associatif et cultuel identifié par Tracfin



Source : Tracfin

D'après le directeur de Tracfin, auditionné par la commission d'enquête, la loi CRPR aurait eu un effet significatif sur le paysage du financement étranger des associations cultuelles. Celui-ci se matérialiserait de façon indirecte par la chute importante des déclarations de soupçons liées à des sujets cultuels ou religieux.

Selon le directeur, le nombre de déclarations de soupçons relatives à ces sujets s'élèverait à 21 653, sans que celles-ci ne concernent forcément des manifestations de séparatisme ou d'ingérence. Néanmoins, depuis l'entrée en vigueur des dispositions concernées de la loi CRPR, ce flux diminuerait sensiblement.

Les origines de cette décrue restent cependant incertaines. Selon le directeur, elles pourraient certes être liées à une diminution de ces pratiques,

à l'augmentation des risques pour les auteurs des infractions, ou au fait que les financements emprunteraient désormais davantage des chemins détournés.

Un agent spécialisé de Tracfin auditionné, dont l'identité est protégée, tend plutôt à défendre la thèse d'un impact positif de la loi CRPR : « *Depuis la promulgation de cette loi, nous constatons collectivement une mise au pas des associations cultuelles, lesquelles donnent des informations de plus en plus exactes. Nous n'avons pas vu passer les "paquets de cash" qui ont été évoqués, et nous observons une diminution des financements en provenance de l'étranger, qu'ils soient déclarés ou non. Ce texte a donc eu un effet de décrue des flux officiels et d'homogénéisation des déclarations, et ce quels que soient les cultes concernés* ».

Le rapport relatif à l'activité de la délégation parlementaire au renseignement (DPR) pour l'année 2022-2023, qui consacre une section à la thématique des ingérences étrangères, fournit des détails supplémentaires à cet égard, en précisant que : « *depuis l'entrée en vigueur de la loi, il ressort que les financements de lieux de culte sur le territoire national émanant de pays du Maghreb, de Turquie et du Moyen-Orient sont en très net recul* »¹.

Enfin, le récent **rapport de la commission des lois du Sénat sur l'application de la loi CRPR**, qui dresse par ailleurs un bilan sévère de l'action du Gouvernement en la matière, considère également que le contrôle des financements étrangers représente « *l'un des points de satisfaction* » de cette loi².

S'agissant du recours **aux cagnottes en ligne**, identifié parmi les points de vulnérabilité, le rapport annuel de Tracfin au titre de 2021 relève que le droit a également connu une évolution positive depuis une ordonnance de 2021³, qui prévoit l'intégration des dispositifs de financement participatif au régime juridique de la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT), qui présente des garanties d'encadrement accrues⁴.

b) Des zones d'ombres subsistent, appelant une vigilance constante des services de renseignement

Le rapport précité de la DPR montre bien que le dispositif ne doit pas dispenser les services de renseignement, aussi bien Tracfin que la DGSI, de maintenir leur vigilance. Selon ce rapport, la DGSI continue d'être chargée, en parallèle, « *de suivre les principaux acteurs d'influence des pays du Maghreb* »

¹ [Rapport public n° 1454 \(Assemblée nationale seizième législature\) / n° 810 – \(Sénat 2022-2023\)](#) fait au nom de la délégation parlementaire au renseignement, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023, déposé le 29 juin 2023.

² [Rapport d'information n° 383 \(2023-2024\)](#) fait par Jacqueline Eustache-Brinio et Dominique Vérien au nom de la commission des lois du Sénat sur l'application de la loi du 24 août 2021 confortant le respect des principes de la République, déposé le 6 mars 2024.

³ Ordonnance n° 2021-1735 du 22 décembre 2021 modernisant le cadre relatif au financement participatif.

⁴ Articles L. 561-1 à L. 561-50 du code monétaire et financier.

de Turquie et des pays du Golfe s'agissant des questions relatives à l'exercice du culte musulman en France, participe au comité de suivi des financements étrangers, piloté par le Coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT). Son rôle consiste à suivre les déclarations des financements étrangers aux niveaux zonal et central, mais également de signaler les financements non déclarés dont elle aurait connaissance par le biais de ses capteurs techniques et humains ».

En outre, ce même rapport relève que l'application du dispositif issu de la loi CRPR a déjà dû conduire les services à prendre des mesures d'entrave. En particulier, il est précisé que Tracfin aurait ainsi « *un certain nombre de mesures d'entrave de l'activité marocaine et algérienne en lien avec la Grande Mosquée de Paris* ».

Par ailleurs, le rapport précité de la commission des lois relève néanmoins que tous les risques n'ont pas disparu pour autant, compte tenu du risque d'une réorientation des opérations d'influences par la voie du financement cultuel, qui pourrait avoir des effets en France par effet de ricochet : ainsi ses rapporteuses « *appellent (...) à ne pas relâcher la vigilance au cours des prochaines années. Selon les informations communiquées par Tracfin, cette réduction des flux en provenance de l'étranger est en effet moins le résultat d'un tarissement stricto sensu que d'une réorientation vers d'autres États, en particulier africains. Dans un contexte d'intrication croissante des économies, ce constat est préoccupant et incite au maintien d'une surveillance active en matière de financements étrangers* ».

c) Des lacunes persistantes identifiées dans les dispositifs issus de la loi confortant le respect des principes de la République par la délégation parlementaire au renseignement subsistent

Le même rapport de la DPR, tout en considérant que la loi CRPR « *a incontestablement emporté des effets positifs par l'apport de nouveaux outils mais aussi par son rôle dissuasif vis-à-vis de certains acteurs qui se sont en effet régularisés de leur propre initiative* », pointe également certaines de ces lacunes.

En premier lieu, son dispositif relatif à l'obligation de déclaration d'intention d'aliéner les locaux cultuels au profit de personnes étrangères ne prend pas en compte les terrains non bâtis. Or, selon la DPR, « *de nombreuses associations poursuivent des projets d'acquisition de terrains afin d'y construire des centres culturels ou des mosquées* ».

En deuxième lieu, cette loi n'aborderait pas la question de la transparence financière des dons et l'appel à la générosité du public. La commission d'enquête relève cependant à cet égard que la réforme du régime applicable aux cagnottes en ligne (voir supra) répond au moins en partie à cet enjeu.

Enfin, la loi ne prévoit pas de dispositif spécifique pour contrecarrer le recours excessif aux sociétés civiles immobilières pour financer et soutenir les associations exerçant le culte. Or, si la loi du 9 décembre 1905

précise que ces associations peuvent détenir des biens immobiliers lorsque cette détention est en lien avec leur objectif social, il apparaît selon la DPR que nombre d'associations cultuelles ne peuvent justifier d'un tel lien.

Le rapport conclue donc que « *la bonne application des nouveaux outils* » de la loi CRPR ne peuvent représenter « *qu'une partie de l'action des services de renseignement* ».

IV. CONCLUSION INTERMÉDIAIRE : LA NÉCESSITÉ D'UNE STRATÉGIE GLOBALE

A. UN BILAN INTERMÉDIAIRE SATISFAISANT : LA FRANCE A CRÉÉ UNE POLITIQUE GLOBALE ET PRIS UNE CERTAINE AVANCE SUR SES PARTENAIRES

1. Une approche globale de la lutte contre les influences étrangères qui couvre, en théorie, l'ensemble des politiques publiques

Depuis 2017 et l'affaire des *Macron Leaks*, la France a manifestement pris la mesure de la menace représentée par les opérations d'influence malveillante, tout particulièrement dans le domaine informationnel. La commission d'enquête ne peut qu'en féliciter. Cette prise de conscience a conduit à élaborer, bloc par bloc, une réponse d'ensemble aux influences étrangères malveillantes. L'ensemble de cette réponse, présentée *supra*, permet de couvrir théoriquement l'ensemble de nos politiques publiques.

Il en ressort un schéma de réponse relativement standardisé, reposant sur trois dimensions.

Premièrement, les actions de détection et de caractérisation regroupent les activités de surveillance et d'identification des opérations d'influence. Par un travail de remontée d'incidents ou de veille systématique, les services en charge de ces actions sont en mesure de repérer l'émergence d'un phénomène d'influence. Il s'agit, par la suite, dans le cadre d'un travail d'enquête, de confirmer ces premiers soupçons, d'identifier l'entité à l'origine de l'opération, sa méthodologie et ses objectifs.

Si l'on prend l'exemple de Viginum, le travail de veille systématique sur les réseaux lui permet d'identifier une activité suspecte, puis, suite à la définition de critères techniques, de lancer une action de collecte et de traitement de données afin de caractériser une ingérence numérique étrangère. Ce travail de caractérisation permet de déterminer si l'opération suspecte découle bien d'une « *diffusion artificielle ou automatisée, massive et délibérée* » de contenus faux ou trompeurs et, dans un second temps, d'attribuer sa conduite à une entité étrangère.

Hors de l'hypothèse d'une opération d'influence menée en ligne, le travail de veille est plus complexe et repose essentiellement sur une remontée

d'information, par des cellules de veille ministérielles dotées d'une spécialisation sectorielle.

Deuxièmement, les actions de riposte correspondent à l'ensemble de la palette d'entraves à la disposition des pouvoirs publics. Comme indiquée dans le deuxième chapitre de la deuxième partie, les mesures d'entrave sont variées et suivent une gradation allant d'un échange diplomatique informel ou une dénonciation publique de l'opération à des mesures de judiciarisation ou à la mise en place d'un régime de sanctions au niveau européen.

À noter que **si certains services n'interviennent que dans une seule dimension**, comme Viginum chargée de la détection et de la caractérisation des ingérences numériques, **d'autres peuvent opérer dans deux dimensions**. C'est le cas de la direction de la communication et de la presse du MEAE qui assure simultanément un travail de veille et des actions de communication stratégique d'entrave.

Troisièmement, en amont de la détection et de la riposte les politiques de résilience visent à protéger la société civile contre les opérations d'influence. Elles permettent d'associer l'ensemble de l'action publique, hors du strict champ des ministères régaliens, à la lutte contre les influences malveillantes. Ces actions, qui interviennent principalement dans la sphère privée, s'appuient logiquement sur la régulation. L'enjeu principal de ces politiques de résilience, s'il n'est pas le seul, est la protection de l'intégrité de l'environnement informationnel, par la régulation des médias et des réseaux sociaux et par des politiques éducatives.

La réponse aux opérations d'influence se répartit entre les différents services compétents selon la sphère visée. **À cet égard, trois champs d'intervention ont pu être distingués :**

- **le territoire et l'espace informationnel français**, comprenant également le champ des activités économiques ;
- **l'image et les intérêts de la France à l'étranger**, qui peuvent également comporter une dimension économique ;
- **le champ des armées**, lié tant au déploiement des forces à l'étranger que l'image des armées.

Dans le cas d'une opération menée sur le territoire français ou ciblant l'espace informationnel français, le travail de détection relève de la direction générale de la sécurité intérieure (DGSI) ou, s'agissant des ingérences numériques ciblant l'espace informationnel français, de Viginum. S'agissant d'opérations d'influence poursuivant un objectif de radicalisation, notamment religieuse, de leurs cibles, le travail de veille relève du comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR). La réponse relève du ministre de l'Intérieur (en particulier de la

DGSI) et, si la réponse donne lieu à des poursuites pénales, le ministre de la Justice.

Si elle concerne toutefois la sécurité économique, la détection relève du Sisse et la réponse du ministre de l'économie et des finances.

Dans le cas d'une opération d'influence visant l'image de la France à l'international, le travail de détection relève de la direction de la communication et de la presse du Quai d'Orsay, et la réponse relève du ministre des Affaires étrangères ou, dans le cadre d'une opération de moindre ampleur, du poste diplomatique compétent avec le soutien de la DCP.

S'il s'agit d'une opération visant des ressortissants français ou des intérêts économiques, la direction générale de la sécurité extérieure est chargée tant du travail de détection que de la riposte, dans le cadre de ses moyens d'action clandestins.

Dans le cas d'une opération d'influence visant les armées, le travail de détection relève du Comcyber si elle concerne l'action des forces françaises sur un théâtre extérieur et de la Dicod si elle porte atteinte à la politique de communication des armées. La direction du renseignement et de la sécurité de la défense (DRSD) intervient également, tant au stade de la détection que de la riposte. La réponse relève du ministre des Armées.

Ces trois sphères ne sont toutefois pas imperméables entre elles. Ainsi, dans l'hypothèse d'une opération d'influence malveillante d'ampleur visant à la fois l'image de la France à l'étranger et les forces armées, les services du ministère de l'Europe et des affaires étrangères et du ministère des armées travaillent de concert dans le cadre de la *task force* interministérielle informationnelle, comme exposé *supra*.

Répartition simplifiée des compétences en matière de détection et de riposte face aux opérations

Cible de l'opération		Travail de détection	Autorité politique chargée de la riposte
Territoire national	Ingérences de toutes natures	DGSI	Ministre de l'intérieur et ministre de la justice (en cas de poursuites pénales)
	Ingérences numériques	SGDSN (Viginum)	
	Influence à des fins de radicalisation	CIPDR	
	Ingérences économiques	SISSE	Ministre de l'économie et des Finances
Étranger	Atteinte à l'image de la France à l'étranger	Direction de la communication et de la presse du MEAE	Ministre de l'Europe et des affaires étrangères
	Ingérence menée contre les ressortissants, entreprises ou intérêts français à l'étranger	DGSE	Ministre des armées
Armées	Lutte d'influence ciblant les forces engagées sur un théâtre extérieur	Comcyber	Ministre des armées
	Atteinte à la politique de communication des armées	Dicod	

Source : commission d'enquête

Par ailleurs, comme présenté tout au long de la deuxième partie du présent rapport, ce schéma de lutte contre les opérations d'influence malveillante en trois temps (détection - riposte - prévention) et dans trois champs (territoire national - étranger - armées) s'appuie sur un corpus législatif et règlementaire relativement complet. La récente loi visant à prévenir les ingérences étrangères en France a permis de pallier les faiblesses de ce corpus, identifiées par le rapport de la commission d'enquête de l'Assemblée nationale sur les ingérences étrangères et par les travaux de la délégation parlementaire au renseignement, dans le champ de la détection (autorisation de la technique dite de l'algorithme), dans le champ de la riposte

(création d'une nouvelle circonstance aggravante pour ingérence et utilisation des techniques d'enquête spéciales et nouvelles compétences pour la HATVP) et dans le champ de la résilience (création d'un répertoire des représentants d'intérêts agissant pour le compte de mandants étrangers).

Aussi, hormis la question du statut des plateformes, dont l'évolution devra être envisagée à moyen terme au niveau de l'Union européenne, **la commission d'enquête n'a identifié aucun manque majeur au sein de notre cadre législatif et règlementaire dans la lutte contre les opérations d'influence.**

Au total, **il est indéniable que la présentation de l'organisation de notre réponse aux influences étrangères malveillantes laisse une impression de foisonnement.** Pour autant, il serait illusoire d'envisager cette politique **comme un jardin à la française, autour d'un organisme unique.** Les influences affectent l'ensemble du champ de nos politiques publiques. **L'étendue de leur impact implique, en outre, que le cœur régional de l'État n'est pas en mesure d'assurer seul la riposte.** En ce sens, Mme Elsa Pilichowski, directrice de la gouvernance publique de l'OCDE, souligne que « *Dans tous les pays, il y a un ensemble d'acteurs. C'est peut-être cela, la bonne pratique internationale. N'avoir qu'un seul acteur paraît impossible au vu de l'étendue et des différents canaux de l'ingérence étrangère. On ne peut pas être spécialisé sur tout. Différentes agences sont chargées de différents aspects. Cela soulève la question de leur coordination* »¹.

2. En comparaison de ses partenaires et alliés, la France dispose d'une certaine avance dans la lutte contre les influences malveillantes

Les auditions et déplacements de la commission d'enquête ont permis d'établir que **la France disposait d'une certaine avance sur ces partenaires et alliés, tant en termes de prise de conscience de la menace au niveau de l'État que de mise en œuvre de dispositifs de réponse.** Seuls les États les plus directement exposés à des stratégies d'influence agressives disposent de politiques de réponse plus développées. Les pays baltes, la Finlande et la Suède, exposées aux manœuvres russes et Taïwan, constamment sous la pression de la Chine, ont adapté leur appareil d'État et se sont dotées de politiques de résilience particulièrement avancées. **En ce sens, le déplacement de la commission d'enquête en Finlande et en Estonie a permis d'identifier plusieurs points dont la France pourrait utilement s'inspirer** (cf. infra troisième partie).

S'agissant du modèle français, Viginum constitue un instrument unique au sein des pays occidentaux : **un service spécifique, dédié à la protection du débat public, sous la surveillance d'un comité éthique, et**

¹ [Audition du 19 mars 2024](#).

disposant de la confiance du public et des journalistes. Ce point mérite d'être souligné. La réussite de l'action publique en matière de lutte contre les influences est en effet conditionnée à une relative confiance des citoyens. Le secrétaire général de la défense et de la sécurité nationale, Stéphane Bouillon, l'a rappelé : « *J'estime que nous sommes à ce titre plus performants que d'autres pays. Les États-Unis et l'Espagne ont échoué à mettre en place un tel dispositif. Pour notre part, nous avons au préalable recueilli les conseils des présidents des assemblées parlementaires et des commissions compétentes au sein de ces dernières, et nous avons fait le tour de tous les dirigeants de tous les partis politiques. De ce fait, le cadre que nous avons posé ne prête pas le flanc à la contestation politique* »¹. Aux États-Unis, l'Agence de cybersécurité et de sécurité des infrastructures², créée en 2018 pour protéger l'infrastructure électorale des ingérences numériques, a en effet été au cœur des débats politiques des élections présidentielles et générales américaines de 2020 et son intégrité remise en cause par une partie de la classe politique comme le chercheuse Maud Quessard l'a indiqué à la commission d'enquête : « *Celle-ci fait l'objet de beaucoup d'attaques car elle a été perçue non pas comme une agence capable de protéger les citoyens américains pour assurer un processus électoral sécurisé mais, au contraire, plutôt pointée du doigt dans le débat public comme étant potentiellement une agence pouvant censurer une partie de la classe politique américaine* »³.

Parmi nos alliés, il existe peu de structures spécifiques ou présentant une forte originalité en matière de lutte contre les opérations d'influence. Deux exemples principaux peuvent être cités. D'une part, le *Global Engagement Center*, placée au sein du département d'État américain, assure à la fois des missions de détection et de divulgation, par la communication stratégique, d'opérations de propagande et de désinformation étrangères (voir encadré *infra*). Ses missions recoupent ainsi à la fois celles de Viginum et celles de la direction de la communication et de la presse du MEAE en France. D'autre part, l'**Agence de défense psychologique suédoise**, créée dans les années 1950 et réactivée en 2022, vise à préserver l'espace informationnel lié aux élections de toute interférence étrangère (voir encadré dans la troisième partie).

Par ailleurs, si la coordination de l'ensemble des services de l'État dans la lutte contre les influences demeure en France un enjeu certain, **le caractère unitaire de l'État français apparaît comme un atout**. Pour la chercheuse Maud Quessard : « *La coordination est un mot clé qui est extrêmement présent partout, et pas simplement pour nos institutions françaises ; à cet égard, nous avons la chance d'être dans un État jacobin par nature plus propice à assurer la coordination qu'un État fédéraliste* »⁴.

¹ [Audition du 11 juin 2024](#).

² Cybersecurity and Infrastructure Security Agency (CISA).

³ [Audition du 7 mars 2024](#).

⁴ *Idem*.

Le *Global Engagement Center* du département d'État américain

Rattaché au département d'État américain, le *Global Engagement Center* (Centre pour la mobilisation mondiale) est une institution de création récente. Il a remplacé en 2016 le Centre de communication stratégique contre le terrorisme¹. La création et les missions initiales du GEC s'inscrivaient dans le contexte de la lutte contre la propagande de *Daech*, justifiant qu'une majorité des agents du centre soient issus des personnels civils et militaires du Pentagone. La loi autorisant le budget de la défense nationale pour l'année 2017 a permis d'étendre son action aux actions de propagande d'États étrangers².

Le GEC est ainsi chargé de détecter, comprendre, exposer et contrer les actions de désinformation et de propagandes d'entités étrangères, étatiques ou non, visant à affaiblir ou influencer les politiques publiques, la sécurité ou la stabilité des États-Unis, de leurs alliés et de leurs partenaires. Pour ce faire, son action s'articule en cinq axes :

- analyse et recherche, une vingtaine de chercheurs et d'analystes collectent des informations sur les tactiques et objectifs d'entités étrangères étatiques et non étatiques ;
- partenariats internationaux, le centre soutient et participe à des coalitions et partenariats internationaux pour renforcer l'environnement informationnel international ;
- programmes et campagnes, quatre équipes, respectivement dédiées à la Chine, à la Russie, à l'Iran et au terrorisme, travaillent pour renforcer la résilience de la société et des institutions face aux menaces informationnelles de ces acteurs ;
- divulgation, le centre assure la coordination interagence pour révéler les campagnes et manœuvres informationnelles visant les États-Unis ou leurs alliés et partenaires ;
- évaluation des technologies, le GEC répertorie et teste les technologies susceptibles d'être utilisées dans la lutte contre la propagande étrangère et la désinformation et d'anticiper la menace de l'utilisation de l'IA générative dans ce domaine.

La défense informationnelle des États-Unis n'est cependant pas l'apanage du seul GEC. Comme le souligne Jean-Baptiste Jeangène Vilmer, le GEC doit coexister avec : « *de nombreuses task forces dédiées à la lutte contre la désinformation et/ou l'influence étrangère, dans d'autres administrations, dont le département de la Justice et le département de la Sécurité intérieure* »³.

Le centre dispose de 70 agents et d'un budget d'environ 170 millions de dollars. Si son action pour contrer la propagande du groupe État islamique s'est révélée relativement efficace, ses résultats sont plus limités s'agissant de la lutte contre les manœuvres de propagande et de désinformation menées par la Russie, la Chine et l'Iran. Selon Maud Quessard, « *le GEC est considéré comme un centre d'analyse de données (data center) peu à même de coordonner des programmes d'information et d'engagement utilisant les moyens humains et cyber* »⁴.

Source : commission d'enquête d'après le site internet du *Global Engagement Center*

¹ *Center for Strategic Counterterrorism Communications*.

² *National Defense Authorization Act for Fiscal Year 2017*.

³ Jean-Baptiste Jeangène Vilmer, « *Chapitre 16. Panorama des mesures prises contre les manipulations de l'information* », in Céline Marangé et Maud Quessard (dir.) *Les guerres de l'information à l'ère numérique*, 2021.

⁴ Maud Quessard, « *Chapitre 10. Les États-Unis : la militarisation de la diplomatie publique* », in Céline Marangé et Maud Quessard (dir.) *Les guerres de l'information à l'ère numérique*, 2021.

B. UN BILAN À PERFECTIONNER : UNE APPROCHE EMPIRIQUE, SANS PORTAGE POLITIQUE INTERMINISTÉRIEL ET INÉGALEMENT MISE EN ŒUVRE SELON LES MINISTÈRES

1. Une approche de la lutte contre les influences qui frappe par son empirisme

En dépit d'un bilan globalement satisfaisant, les politiques de lutte contre les opérations d'influences malveillantes frappent par leur empirisme. Les différents instruments de détection et de riposte sont nés en réponse aux opérations d'influence ayant visé la France depuis 2017. Cinq faiblesses ressortent de cet empirisme.

Premièrement, on constate une véritable « archipelisation » des capacités de détection et de caractérisation, au risque d'un fonctionnement en silos et d'une dispersion des moyens. De nombreux ministères, confrontés à l'émergence d'opérations d'influence dans leurs champs d'action, se sont dotés de capacités de détection et de caractérisation. Si cette floraison de cellules de veille et de *task forces* permet une plus grande couverture du champ des politiques publiques, il est indispensable d'assurer une plus grande communication et une remontée de l'information.

Deuxièmement, le phénomène des influences étrangères demeure relativement mal connu académiquement. Les différentes auditions d'universitaires et de chercheurs, spécialistes des questions informationnelles, de la Russie, des États-Unis et de l'islam, ont unanimement souligné le manque de moyens de la recherche en sciences sociales.

Troisièmement, il n'existe pas, sur le plan stratégique, de vision unifiée sur la question des influences étrangères ni, sur le plan opérationnel, de doctrine de réponse clairement définie aux manœuvres hostiles.

Quatrièmement, le portage politique de la question des influences étrangères est inexistant au niveau interministériel. La doctrine implicite de réponse aux opérations d'influence repose sur le ministre compétent au fond, qui assure dès lors la dénonciation, l'arbitrage portant sur la réponse pouvant remonter jusqu'au Président de la République. Toutefois, le niveau interministériel et singulièrement le Premier ministre sont absents de cette équation. Il n'existe pas de « guichet unique » politique en matière d'influence, en mesure de mobiliser les services de l'État, y compris hors du domaine régional. Dès lors, seuls les ministères les plus concernées sectoriellement s'investissent pleinement dans la lutte contre les influences malveillantes.

Cinquièmement, la société civile n'est nullement associée par l'État à la lutte contre les influences malveillantes. Hormis des initiatives ponctuelles improvisées par les services compétents, les ressources de la société civile demeurent peu exploitées et les citoyens mal sensibilisés à la

menace. Cette omission est d'autant plus paradoxale que la société est la cible principale des opérations d'influence qui cherchent, au travers de manœuvres informationnelles, à saper sa cohésion.

L'apparente improvisation des services de l'État pour construire une réponse aux opérations d'influence malveillante n'est pas inquiétante en soi. Le domaine est relativement nouveau et la France a su agir pour établir une politique cohérente, plus rapidement et plus efficacement que nombre de ses alliés. Dans le domaine cyber, la formalisation d'une stratégie nationale en 2021 est intervenue en aval de la construction. Pour autant la commission d'enquête, à l'issue de ses travaux, estime que cet empirisme doit être dépassé pour construire une stratégie cohérente de réponse à la menace des influences.

2. Un décalage inquiétant entre la sphère régaliennes et le reste des services de l'État sur la prise en compte de la menace des influences malveillantes

La commission d'enquête a pu constater que **si le cœur régalien de l'État est pleinement au fait des enjeux liés aux influences étrangères, le reste des ministères est encore peu impliqué dans cette politique.**

La problématique des influences malveillantes n'est pourtant pas ignorée par les administrations non régaliennes. Les travaux parlementaires ont ainsi contribué à alerter les ministères sur le décalage existant entre l'état de menace et l'absence de dispositifs de détection et de caractérisation efficents. Dans le domaine de l'enseignement supérieur et de la recherche, le rapport d'information du sénateur André Gattolin¹ a souligné les faiblesses du dispositif de protection du potentiel scientifique et technologique de la Nation et formulé des recommandations visant pallier ces faiblesses.

Pour autant, en dépit de ces alertes, les dispositifs de veille et d'alerte, hors du domaine régalien, paraissent encore insatisfaisants à la commission d'enquête. C'est par exemple le cas dans le domaine universitaire. Benjamin Leperchey, adjoint à la direction générale de l'enseignement scolaire et de l'insertion professionnelle, a ainsi indiqué à la commission d'enquête que « *Les opérations sont actuellement beaucoup moins frontales, ce qui rend les frontières plus floues, si bien que les mécanismes de recensement et de détection que le rapport du Sénat de 2021 nous encourageait à faire progresser restent difficiles à mettre en œuvre* »². De plus, le constat de la menace est encore imparfaitement pris en compte par les responsables publics : « *Il n'y a pas de naïveté sur le sujet, mais la prise de conscience reste hétérogène parmi les présidents d'établissement* »³. L'implication des autorités chargées de la

¹ [Rapport d'information n° 873 \(2020-2021\)](#) fait par André Gattolin au nom de la mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences, déposé le 29 septembre 2021.

² [Audition du 2 mai 2024](#).

³ *Idem.*

régulation est également inégale. S'agissant de l'Arcom, son président, Roch-Olivier Maistre a clairement indiqué que la surveillance des médias en langues étrangères diffusés en France était contrainte par le manque de moyens de l'autorité : « *Ce travail est nécessairement contraint par les ressources qui sont les nôtres. Nous cherchons donc à cibler au mieux nos contrôles. Si nous étions saisis d'un volume plus significatif que les quelques chaînes de télévision que j'ai évoquées, cette contrainte serait certainement difficile à gérer en termes de moyens – je tiens à le souligner* »¹.

Ensuite, le maillage territorial des mécanismes de détection demeure incomplet. En matière économique, les délégués du Sisse ne sont placés qu'auprès des préfets de région, ne permettant pas de contrôler l'ensemble des activités économiques sur le territoire ni de véritablement assurer une mission de sensibilisation des entreprises stratégiques. En matière universitaire, si le réseau des fonctionnaires de sécurité et de défense (FSD) couvre théoriquement l'ensemble des établissements d'enseignement supérieur et de recherche, le cumul des fonctions de FSD avec d'autres fonctions administratives ne permet pas une véritable professionnalisation. De plus le réseau de veille et d'alerte du service de défense et de sécurité ne couvre pas les établissements d'enseignement supérieur privés.

Enfin, la commission d'enquête estime que les potentialités offertes par la société civile ne sont pas pleinement mobilisées par les pouvoirs publics. Or, comme il sera exposé *infra* dans la troisième partie, la lutte contre les influences implique d'associer les différentes composantes intéressées, journalistes et chercheurs, et de sensibiliser plus largement le secteur privé et la population.

¹ [Audition du 19 mars 2024](#).

TROISIÈME PARTIE : POUR UNE POLITIQUE PUBLIQUE DE LUTTE CONTRE LES INFLUENCES ÉTRANGÈRES MALVEILLANTES FONDÉE SUR TROIS PILIERS

Au terme de ses travaux, et sans remettre en cause les initiatives bienvenues et les progrès importants réalisés par les pouvoirs publics dans les années récentes rappelés dans la partie précédente, la commission d'enquête préconise une refonte globale de notre approche collective du phénomène des influences étrangères malveillantes.

Avant toute chose, il nous faut prendre collectivement conscience du fait qu'*in fine*, l'efficacité des opérations d'influence étrangères malveillantes est seulement celle que la population lui donne. À la différence de pays exposés de longue date aux manipulations de l'information, notamment d'origine russe, la société française paraît, à cet égard, encore trop naïve. Il importe à cet égard, d'une part, de se donner les moyens de mesurer l'impact réel de ces opérations et, d'autre part, de prendre acte que la lutte contre les influences étrangères est l'affaire de tous, les responsables publics comme les citoyens. Elle ne peut pas rester l'apanage de l'État : si les dispositifs de protection, de détection et de riposte que celui-ci met en place sont évidemment nécessaires, ils ne sauraient se substituer à l'effort d'édification d'une société véritablement résiliente.

En deuxième lieu, la posture défensive, et partant essentiellement passive, qui a jusqu'ici été la nôtre face aux influences étrangères malveillantes a montré ses limites. Il est désormais nécessaire d'assumer une véritable politique d'influence positive défendant les valeurs et les intérêts français auprès des opinions publiques internationales, et de s'engager ainsi pleinement dans la bataille des narratifs, qui détermine la « *bataille des perceptions* ». Cela nous impose de nous donner les moyens de produire des narratifs à la fois efficaces et authentiques. Pour une démocratie comme la nôtre, il serait en effet inenvisageable d'utiliser l'arme de la désinformation, comme le font nos compétiteurs.

En troisième et dernier lieu, il appartient dans ce contexte à l'État de prendre ses responsabilités en se dotant d'une stratégie globale et interministérielle de lutte contre les influences étrangères malveillantes, dans le but d'ordonner son action et ainsi mettre un terme à l'empirisme qui a dominé au cours des dernières années. Cette stratégie, qui devra intégrer pleinement les exigences serait structurée « *en cercles concentriques* », en comprenant un premier volet strictement régional, un deuxième volet dédié aux politiques sectorielles concourant à la lutte contre les influences étrangères malveillantes, et un dernier volet, transversal et inclusif dédié aux

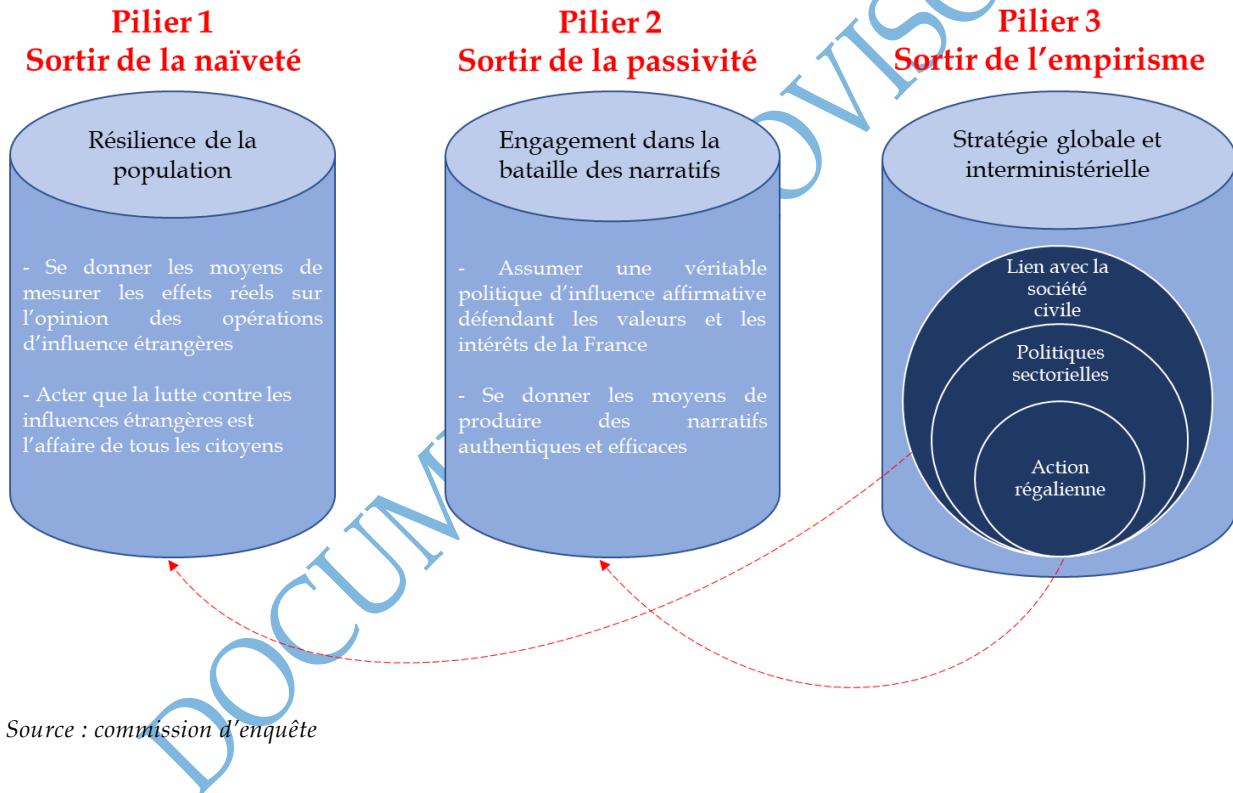
actions en direction de la société civile ainsi qu'à l'intégration de ses initiatives, de façon renforcer notre résilience collective.

Sortir de la naïveté, sortir de la passivité et sortir de l'empirisme : tels sont les trois piliers de la feuille de route préconisée par la commission d'enquête pour réussir la refondation qu'elle appelle de ses vœux.

La section I de la présente partie présente successivement les objectifs poursuivis dans le cadre de ces trois piliers.

Les sections II à IV déclinent ensuite, pour chaque « cercle » précité, les principales mesures opérationnelles pouvant être prises par l'État dans le cadre de sa stratégie de lutte contre les influences étrangères malveillantes.

Refondation de notre approche collective de la lutte contre les influences étrangères malveillantes : une feuille de route reposant sur trois piliers



I. LA NÉCESSITÉ DE REFONDER NOTRE APPROCHE COLLECTIVE DU PHÉNOMÈNE

A. PREMIER PILIER : SORTIR DE LA NAÏVETÉ, ET ACTER QUE LA LUTTE CONTRE LES INFLUENCES ÉTRANGÈRES MALVEILLANTES EST L'AFFAIRE DE TOUS

1. À court terme, la nécessité de mesurer l'impact des opérations d'influence étrangères et de nous donner les moyens d'assurer son suivi dans la durée

a) L'importance de ne pas « crier avant d'avoir mal »

À la fin, l'efficacité des opérations d'influence étrangères malveillantes est celle que les populations qui en sont les cibles leur donnent. D'où l'importance de mesurer le plus finement possible leur impact.

L'un des écueils auquel nous risquerions d'être confrontés serait de surestimer leur impact.

Comme le rappelle Laurent Cordonier, directeur de recherche à la fondation Descartes auditionné par la commission d'enquête : « être exposé à une désinformation ou à un contenu de propagande et d'influence, ne signifie pas nécessairement adhérer ou croire à cette désinformation : l'exposition n'équivaut pas à l'adhésion ou à la croyance »¹.

Pour mémoire, celui-ci indique à ce titre **trois facteurs de sensibilité individuelle** à la désinformation (voir *Première partie, III, E*) :

- le « *style de pensée* », qui peut être plus intuitif ou plus analytique, le premier étant davantage sensible à la désinformation ;
- le **manque de connaissances de qualité** sur le sujet concerné par la désinformation ;
- le **niveau de défiance à l'égard des sources d'informations fiables et des institutions**.

Or, en la matière, « *crier avant d'avoir mal* » pourrait avoir des conséquences délétères. Le simple fait que nous puissions croire en l'efficacité des opérations d'ingérences informationnelles et en leur capacité effective à altérer les processus électoraux suffirait à atteindre les objectifs de nos compétiteurs, puisque cela reviendrait à reconnaître l'extrême faiblesse de notre modèle démocratique. Pire, si, pour lutter contre une menace surévaluée, nous étions conduits à mettre en place des dispositifs de protection ou de riposte portant une atteinte disproportionnée aux libertés ou contraires aux valeurs démocratiques, nous achèverions de leur donner la victoire.

¹ [Audition](#) du 7 mars 2024.

À cet égard, Julien Nocetti, chercheur au Centre d'analyse, de prévision et de stratégie auditionné par la commission d'enquête soulignait bien que : « *Les discours alarmistes peuvent susciter une forme d'anxiété au sein de la population. Cependant, le bruit médiatique autour de ces sujets est l'un des objectifs des acteurs propagéant des manipulations d'information. On risque d'offrir une chambre d'écho aux manœuvres hostiles, souvent russes, voire de favoriser une forme de soutien vis-à-vis de la restriction de la liberté d'expression en ligne et, à plus long terme, de contribuer au désenchantement vis-à-vis de la démocratie* »¹.

b) Soutenir la recherche académique pour mesurer le phénomène le plus finement possible

Pour Paul Charon, chercheur à l'Institut de recherche stratégique de l'École militaire auditionné par la commission d'enquête, « *sur les problématiques d'ingérences, d'influence, de manipulations de l'information, l'un des points aveugles de la recherche concerne l'efficacité des opérations. À quel moment une opération est-elle efficace ? En quoi ? À quel degré ? Pourquoi certaines le sont-elles et d'autres non ? Nous manquons de capacités à évaluer l'efficacité réelle des opérations. C'est évidemment l'un des axes à améliorer dans les années à venir* »².

Une autre spécialiste, le professeur Divina Frau-Meigs, pointe clairement un « *déficit de connaissances* » en la matière³, et souligne les tendances contradictoires qui traversent le champ académique dans ce domaine.

Cette dernière commence en effet par relever que les recherches portant sur la France, qui se sont concentrées sur les opérations de désinformation menées dans le contexte de la campagne électorale de 2017 concluaient à « *la faible présence d'infox pendant la campagne* » qui « *tendent à être cantonnées à leur communauté* », de sorte que leur audience serait « *très restreinte* »⁴.

Dans le même temps, elle alerte sur le fait que, selon elle, « *la plupart des recherches minimisent l'effet direct de la désinformation, et mettent en avant la difficulté à établir une jauge de l'influence car l'exposition ne vaut pas l'engagement ou la conviction* », mais que « *il n'existe pas encore une masse critique de travaux pour pouvoir se prononcer sur les effets diffus et à long terme* ». Elle poursuit : « *la recherche sur les effets de la violence à la télévision montre que les cas d'intimidation directe sont peu nombreux, quoique spectaculaires* », mais le sentiment de peur et d'insécurité augmente. De même, pour la désinformation, où le changement de comportement lors d'un scrutin (abstention ou adhésion populiste) semble moins à

¹ [Audition](#) du 4 juin 2024.

² [Audition](#) du 6 juin 2024.

³ Divina Frau-Meigs, « *Les enjeux de la réception : comment mesurer l'influence de la désinformation* » in Céline Marangé et Maud Quessard (dir.), *Les guerres de l'information à l'ère numérique*, Presses universitaires de France, janvier 2021, p. 325.

⁴ Divina Frau-Meigs, op. cit., p. 326-327.

redouter que le soupçon généralisé et l'érosion de la confiance dans les institutions démocratiques »¹.

Pour illustrer cette problématique, un agent public de Viginum auditionné par le rapporteur a utilisé la métaphore de la mer s'échouant sur la falaise : si quelques vagues de désinformation est peu susceptible de produire des effets massifs, à terme, leur multiplication et leur banalisation finir inexorablement par éroder la roche. Encore faut-il mesurer sous quelles conditions et selon quelle temporalité ce phénomène se produit en pratique.

Pour ces raisons, la commission d'enquête considère que le soutien à la recherche académique sur l'impact et perception et la réception des opérations de manipulation de l'information sur l'individu et la société doit être érigé en priorité par le ministère chargé de l'enseignement supérieur et de la recherche.

Pour appréhender le phénomène sous toutes ses dimensions, cet effort devra nécessairement être conduit de façon transdisciplinaire, et associer des experts en sociologie, science politique, relations internationales, sciences cognitives, psychologie, technologies de l'information et de la communication *etc.*

Une telle initiative pourrait prendre la forme d'appels à projets susceptibles d'être lancés et financés sans délai par l'Agence nationale de la recherche (ANR).

De tels appels à projets pourraient être relancés de façon régulière, afin que nos connaissances sur cette matière en évolution constante du fait des évolutions technologiques puissent être dûment mises à jour.

Recommandation n° 1 : Engager sans délai des recherches académiques transdisciplinaires sur la perception et la réception des opérations de manipulation de l'information sur l'individu et la société, et veiller à l'actualisation régulière de nos connaissances en la matière.

2. À plus long terme, bâtir une société résiliente où chacun se considère acteur de sa protection et de celle des autres

Pour la commission d'enquête, le premier et principal objectif que nous devons collectivement nous fixer est celui d'assurer, à long terme, la résilience de notre Nation face aux opérations d'influence étrangères.

¹ *Divina Frau-Meigs*, op. cit., p. 342-343.

Le ministre Jean-Noël Barrot, lors de son audition, a proposé une analogie entre les ingérences numériques étrangères et un « *virus* », fonctionnant « *par contaminations successives des citoyens entre eux* ». S'il est important de les détecter et les traiter, le plus crucial est bien de « *développer l'immunité* »¹.

Plusieurs leviers de politique publique peuvent être mobilisés à cette fin à court et moyen termes :

- premièrement, une amélioration de la qualité de l'environnement informationnel est indispensable, et doit conduire à se fixer comme objectif la promotion de contenus fiables, en particulier sur les plateformes numériques ;

- deuxièmement, une **sensibilisation et une formation de l'ensemble des composantes de la population à la problématique des influences étrangères est nécessaire**. Comme l'a expliqué le journaliste Thomas Huchon lors de son audition : « *avoir conscience qu'il existe de potentielles manipulations constitue en effet une première manière de se protéger. Une communication publique doit faire état de ces potentiels dangers, comme on pourrait parler des dangers d'une substance illicite ou de comportements routiers inappropriés, afin de conduire à une position claire sur l'éducation aux médias, à l'information et au décryptage de l'information, laquelle devrait devenir de l'ordre du savoir fondamental enseigné à l'école dès le plus jeune âge* »² ;

Des chantiers de long terme et de portée plus large, excédant pour partie le champ de la commission d'enquête, doivent également être considérés à l'aune de leur effet bénéfique sur la résilience de la société.

En premier lieu, le **développement de l'esprit critique** des citoyens joue un rôle majeur.

Pour Laurent Cordonier, celui-ci comporte deux principaux volets :

« *D'une part, il s'agit de prendre conscience de notre état de dépendance épistémique totale : nos propres sens et nos propres expériences étant limitées, nous connaissons le monde essentiellement par le biais du témoignage d'autrui. Si je sais aujourd'hui qu'il y a une guerre en Ukraine, c'est parce que des journalistes sur le terrain me l'ont rapporté. Quand on fait la liste de ce que l'on sait par soi-même, on réalise qu'elle est limitée et qu'on est donc presque toujours dépendant du témoignage d'autrui. Dans ces conditions, le facteur de la connaissance est celui de la confiance et, par ricochet, on peut comprendre que le nerf de la guerre, au niveau individuel, est d'être capable d'attribuer à bon escient sa confiance sur des bases rationnelles plutôt que sur des bases potentiellement émotionnelles, ou d'habitude, etc.* »

La seconde composante de l'esprit critique « *réside dans la compréhension du fonctionnement de notre esprit. Nous sommes tous influencés par des biais cognitifs (...), c'est-à-dire des raccourcis qui nous permettent souvent de gagner du temps pour nous faire une opinion sur un sujet ou comprendre une*

¹ [Audition](#) du 29 mai 2024.

² [Audition](#) du 9 avril 2024.

situation, mais qui, dans un certain nombre de cas, nous mènent à commettre des erreurs systématiques. Je ne prendrai qu'un seul exemple, celui du biais de confirmation : on a tous tendance à favoriser les informations qui vont dans le sens de ce que l'on sait déjà. Une fois que l'on en prend conscience, quand on fait une recherche Google, il devient quasiment impossible de se demander : "ne suis-je pas juste en train d'essayer de confirmer ce que j'ai envie de croire et ce que je sais déjà ?", et donc là, au niveau individuel, on se place dans une attitude qui nous permet potentiellement de ne pas être piégés par notre propre système cognitif. ¹»

En deuxième lieu, **tout ce qui concourt à retisser un lien de confiance entre les médias, les institutions et la population** participe à l'amélioration de la résilience de cette dernière face aux opérations d'influence étrangère.

Enfin, de façon plus structurelle encore, il est essentiel de garder à l'esprit que les opérations d'influence étrangères malveillantes selon une logique de « puissance tranchante » (voir *Introduction*), instrumentalisent, notamment grasses à de fausses informations, des fractures de notre société qui, elles, sont bel et bien réelles (voir *Première partie, II*). Ainsi, **de même, tout ce qui concourt à améliorer la cohésion nationale**, à réduire les inégalités sociales et environnementales ainsi qu'à apaiser les tensions identitaires, renforce d'autant notre résilience.

In fine, le modèle de société vers lequel nous devons nous efforcer de tendre est celui d'une société dans laquelle chacun se considère comme acteur de sa protection et de celle des autres. Dans cette perspective, chacun s'astreindrait à une certaine discipline dans son rapport à l'information, en s'efforçant de vérifier les informations qu'il reçoit, en particulier avant de prendre la décision de les partager ou les diffuser.

Des sociétés exposées de longue date aux ingérences informationnelles, telles que celles des **pays baltes et nordiques**, ciblés par la Russie ou encore de **Taiwan**, ciblé par la Chine, constituent un modèle en la matière. À Taiwan, une initiative telle que le programme public « *Humor against rumor* » (« *L'humour contre les rumeurs* ») mis en place durant la crise de la Covid-19 et visant à répondre avec humour aux opérations de désinformation circulant au sujet du virus témoigne d'une certaine maturité de la population sur ces questions, dont nous ne pouvons que nous inspirer. Le déplacement effectué par la délégation de la commission d'enquête en Finlande et en Estonie inspire également les recommandations contenues dans la section IV de la présente partie, relatives à la résilience de la société.

¹ [Audition](#) du 7 mars 2024.

B. DEUXIÈME PILIER : SORTIR DE LA PASSIVITÉ, ET ASSUMER UNE VÉRITABLE POLITIQUE D'INFLUENCE AFFIRMATIVE PORTEUSE DE NARRATIFS DÉFENDANT LES VALEURS ET LES INTÉRÊTS FRANÇAIS

La commission d'enquête considère qu'il nous faut **rompre avec une posture défensive, et partant essentiellement passive, qui a jusqu'ici été la nôtre face aux influences étrangères**. Il est désormais nécessaire d'assumer une véritable politique d'influence affirmative défendant les valeurs et les intérêts français auprès des opinions publiques internationales.

Le présent rapport a évoqué *supra* (voir *Deuxième partie, II*) les lacunes de la politique d'influence française actuelle.

Plusieurs initiatives témoignent certes d'une prise de conscience de la nécessité de la renforcer, au premier rang desquelles :

- la mise en place d'une *task force* informationnelle interministérielle (TF2I) co-animée par la direction de la communication et de la presse du ministère des Affaires étrangères et le pôle « Anticipation stratégique et orientations » (ASO) au sein de l'état-major des armées ;
- l'adoption d'une Stratégie nationale d'influence (SNI).

Cette dernière comporte toutefois des certaines limites, également détaillées *supra*. De surcroit, le caractère très tardif de son élaboration (printemps 2024), soit près de deux ans après la consécration de la « *fonction influence* », qui en est à l'origine, dans le cadre de la Revue nationale stratégique 2022¹, illustre bien la difficulté des pouvoirs publics à pleinement s'emparer de cet enjeu.

Adopter une posture affirmative constitue pourtant une nécessité, alors que la « *bataille des narratifs* », pour reprendre l'expression employée par le général Ianni, directeur du pôle ASO lors de son audition par la commission d'enquête², est désormais au cœur de la compétition stratégique mondiale.

Notre réussite en la matière, soit le développement de notre « *pouvoir discursif* » (voir *Introduction*) pourra être mesurée à l'aune d'une double exigence :

- notre **capacité à produire des narratifs authentiques et loyaux**, défendant les intérêts français sans chercher à nuire aux autres États, sans chercher à désinformer leurs habitants ou à déstabiliser leurs sociétés ;
- notre **capacité à produire des narratifs efficaces**, ce qui suppose d'évaluer et de renforcer adéquatement notre diplomatie publique, en étant en mesure d'adapter chacun de nos messages à leurs destinataires. Le travail conduit par Anne-Sophie Avé, Ambassadrice pour la diplomatie publique en

¹ Secrétariat général de la défense et de la sécurité nationale, [Revue nationale stratégique 2022](#).

² [Audition](#) du 2 mai 2024.

Afrique auditionnée par la commission d'enquête¹, a par exemple permis de mettre en évidence un certain nombre de conditions pour garantir l'efficacité de notre communication dans ce continent.

Pour autant, la politique d'influence affirmative que la commission d'enquête appelle de ses vœux ne peut pas tout.

En effet, il importe de souligner que, de même que l'efficacité des opérations de manipulations de l'information menées sur le territoire français est corrélée à la vigueur des fractures sociales qu'elles instrumentalisent, le succès opérations menées à destination des opinions publiques de pays étrangers demeure étroitement lié aux failles structurelles de notre propre politique internationale. Comme l'a par exemple souligné le capitaine de vaisseau Yann Briand, sous-directeur des affaires internationales du secrétariat général de la défense et de la sécurité nationale (SGDSN) concernant la situation au Sahel, « *l'existence, parmi certaines populations africaines, d'un sentiment anti-français ne se réduit pas à une manipulation de l'information par Wagner ; il peut exister des raisons plus profondes. Il faut donc traiter ces problèmes comme une menace hybride, mais également comme une véritable question politique* »².

Ainsi, si un renforcement de notre politique d'influence affirmative est bien indispensable pour faire face aux opérations d'influence étrangères malveillantes menées contre nous, il convient dans le même temps de garder à l'esprit qu'elle ne nous dispense pas d'œuvrer à une amélioration de nos relations diplomatiques stratégiques, bien que ce chantier excède le champ de la commission d'enquête.

Par ailleurs, **le rayonnement de la France dans ne dépend pas uniquement des narratifs développés par les autorités françaises. Notre audiovisuel extérieur, porté en toute indépendance du Gouvernement par France Médias Monde, en assumant une véritable mission de service public international, concourt pleinement à la défense des valeurs de la France et de la démocratie**, selon les mots de sa présidente-directrice générale, Marie-Christine Saragosse lors de son audition en offrant « *une information libre et indépendante, vérifiée sur le terrain si cela est possible* » en portant « *les valeurs démocratiques et les principes humanistes qui caractérisent notre pays* », en promouvant « *le français et la francophonie, tout en respectant et en mettant en valeur les autres langues* » ; en accompagnant des médias locaux, par des actions de coopération et de formation, « *car plus il y aura de médias indépendants et libres, plus les écosystèmes démocratiques pourront être soutenus* »³.

¹ [Audition](#) du 30 avril 2024.

² [Audition](#) du 27 février 2024.

³ [Audition](#) du 6 juin 2024.

C. TROISIÈME PILIER : SORTIR DE L'EMPIRISME, ET DOTER L'ÉTAT D'UNE STRATÉGIE GLOBALE, NATIONALE ET INTERMINISTÉRIELLE DONT LA MISE EN ŒUVRE SERAIT ASSURÉE PAR UNE GOUVERNANCE ADAPTÉE

1. De multiples initiatives doctrinales et stratégiques ont été prises dans les années récentes où sont en voie de l'être

Il n'existe pas, en l'état, de stratégie globale, nationale et interministérielle de lutte contre les influences étrangères malveillantes.

Plusieurs documents stratégiques ont cependant été élaborés dans les années récentes ou sont en voie de l'être.

En la matière, le **SGDSN** a également produit un bref document de référence sur les stratégies hybrides, que la commission d'enquête s'est procuré. Son champ excède largement celui des influences étrangères, abordées sous le seul angle des manipulations de l'information.

Les armées ont été précurseurs, avec l'adoption, dès 2021, d'éléments publics de doctrine de lutte informatique d'influence (L2I)¹ découlant de la Vision stratégique du chef d'état-major des armées².

De son côté, le **ministère des affaires étrangères** a publié en 2022 sa Feuille de route de l'influence³, puis, plus récemment, a élaboré en 2024 la Stratégie nationale d'influence prévue par la Revue nationale stratégique 2022, que la commission d'enquête s'est procurée.

Enfin, il est à noter que la direction des affaires criminelles et des grâces (DAGC) du **ministère de la justice** a diffusé auprès des juridictions dès 2021 un document de politique pénale dédié à la lutte contre les ingérences étrangères prenant la forme d'un « *Focus* » présentant de façon synthétique le régime juridique applicable aux infractions pénales afférentes.

Plusieurs chantiers sont par ailleurs en cours :

- au sein de l'état-major des armées, le pôle ASO pilote la **structuration d'une aptitude interarmées « influence et lutte informationnelle » (ILI)**, décrite à ce stade dans un document de doctrine non public. Dans ses réponses au questionnaire du rapporteur, l'état-major des armées a indiqué que « *la poursuite du développement au niveau des armées d'un corpus doctrinal cohérent et robuste est en cours* », en vue de l'élaboration d'une véritable stratégie ILI qui serait déclinée en feuilles de route régionales et thématiques ;

¹ Ministère des armées, [Éléments publics de doctrine militaire de lutte informatique d'influence \(L2I\)](#), octobre 2021.

² [Vision stratégique du chef d'état-major des armées](#), octobre 2021.

³ Ministère de l'Europe et des affaires étrangères, [Feuille de route de l'influence](#), 2022.

- au niveau du SGDSN, une lettre de mission a été signée par le Premier ministre pour l'élaboration d'une revue stratégique dédiée à la lutte contre les manipulations de l'information (LMI).

En dehors du champ régional, la commission d'enquête a constaté qu'aucun ministère n'a produit de document stratégique consacré à la lutte contre les influences étrangères, alors même que plusieurs d'entre eux sont au cœur des enjeux ayant trait à la résilience de la nation. On peut notamment penser aux ministères chargés de la culture, de l'éducation nationale, de la jeunesse et des sports, ou encore de l'enseignement supérieur et de la recherche.

Tout au plus, certaines initiatives locales ont pu être prises, mais en dehors de tout pilotage ou portage politique ministériel, à l'instar du plan mis en place par l'Inalco pour détecter les opérations d'influence étrangères depuis la fin de l'année 2023 (voir *Deuxième partie, III*).

En synthèse, aucun document stratégique appréhendant le phénomène des influences étrangères malveillantes dans sa globalité et prévoyant les politiques publiques à conduire pour y répondre dans le périmètre interministériel large qui s'impose au vu du caractère extrêmement diffus de la menace.

2. Élaborer une véritable stratégie globale, nationale et interministérielle de lutte contre les influences étrangères

a) Une double exigence de globalité et d'interministérialité

La commission d'enquête considère que le temps est venu de sortir de l'empirisme. La multiplication des dispositifs et des initiatives doctrinaires depuis 2021 a marqué une prise de conscience salutaire, mais ne constitue pas une garantie d'efficacité pour l'action publique, qui doit concerner l'ensemble du champ interministériel.

Dans le domaine de la cybersécurité, après la création de l'Agence nationale de la sécurité des systèmes d'information (Anssi), il a fallu attendre douze ans pour que l'État se dote en 2021 d'une véritable stratégie nationale cyber. Compte tenu de la menace, en particulier dans l'espace informationnel, nous ne pouvons pas nous permettre d'attendre aussi longtemps dans le domaine de la lutte contre les influences étrangères malveillantes.

Cette stratégie doit satisfaire une **double exigence** :

- être réellement globale, en appréhendant le phénomène de la lutte contre les influences étrangères malveillantes à travers l'ensemble de ses manifestations, qui intègrent naturellement les opérations de manipulation de l'information, notamment dans l'espace numérique, mais également les autres types d'opérations d'influence : opérations visant l'enseignement supérieur et la recherche, capture des élites, instrumentalisation des diasporas, opérations d'influence dans le domaine économique... ;

- être pleinement interministérielle, en associant non seulement les ministères régaliens (armées, affaires étrangères, intérieur et justice) mais également l'ensemble des ministères susceptibles d'être concernées par la menace ou mobilisées dans la lutte contre celle-ci (culture, éducation nationale, jeunesse et sports, vie associative, enseignement supérieur, recherche,), ainsi que les politiques publiques de régulation pertinentes (communication, transparence de la vie publique, financement de la vie politique...). Cette action interministérielle devrait elle-même être menée en lien avec les collectivités territoriales, les corps intermédiaires, la société civile (médias, chercheurs...)

Cette stratégie aurait ainsi vocation à regrouper et rationaliser l'ensemble de la production doctrinale et stratégique mentionnée *supra*.

Pour bâtir sa stratégie, la France pourrait notamment s'inspirer de l'Australie, qui a mis en place, dès 2019, une stratégie nationale de contre-ingérence¹.

¹ [Australia's Counter Foreign Interference Strategy](#).

La stratégie nationale australienne de contre-ingérence

La stratégie nationale australienne de contre-ingérence (*Australia's Counter Foreign Interference Strategy*) a été mise en place en 2019.

Elle repose sur le constat que « *les ingérences étrangères et l'espionnage constituent le principal enjeu de sécurité pour l'Australie* ». Le pays est en effet la cible constante d'opérations d'influence de la Chine, dans un contexte d'agressivité croissante de la posture chinoise dans l'Indopacifique.

Pour autant, la stratégie s'affiche clairement comme neutre vis-à-vis des pays à l'origine des opérations d'ingérence, et se concentre sur un objectif de renforcement de la résilience des secteurs de la société australienne identifiés comme étant les plus à risque (gouvernement, universités, industries, médias, collectivités territoriales).

La stratégie de contre-ingérence regroupe l'ensemble des acteurs australiens individus, institutions et gouvernements (fédérés et fédéral), industrie, monde universitaire, médias, communautés.

En matière de coordination, l'Australie s'est dotée en 2018 d'un coordinateur national de la contre-ingérence (*National Counter Foreign Interference Coordinator*). Celui-ci est soutenu par un centre de coordination de la contre-ingérence (*Counter Foreign Interference Coordination Center*) chargé de coordonner les efforts déployés par l'ensemble du gouvernement australien pour répondre aux actes d'ingérence étrangère :

Le coordinateur national a pour mission :

- d'appliquer la stratégie de lutte contre l'influence étrangère en créant un programme national et international intégré et coordonné de lutte contre les ingérences étrangères ;
- de coordonner les efforts de sensibilisation et les conseils aux secteurs menacés ;
- de renforcer l'engagement auprès des communautés étrangères installées en Australie afin de les aider à lutter contre la manipulation par des acteurs étrangers.

Source : commission d'enquête, d'après les réponses de l'Ambassade de France en Australie au questionnaire du rapporteur

b) Privilégier la notion « *d'influences étrangères malveillantes* » à celle d'ingérence

Pour élaborer cette stratégie, il conviendra de se référer à la notion d'« *influences étrangères malveillantes* », qui paraît ici préférable à celle d'ingérence, et ce pour plusieurs raisons.

En effet, l'influence constitue une finalité, là où l'ingérence constitue un procédé (voir *Introduction*).

Pour les besoins de l'élaboration d'une telle stratégie, la notion d'ingérence est à la fois trop large et trop restrictive : trop large, dans la

mesure où les ingérences peuvent poursuivre d'autres finalités que l'influence (cyberattaques, mobilisation de l'arme normative, ingérences économiques sans finalité d'influence...), et trop restrictive, dans la mesure où l'ingérence ne vise que des opérations dissimulées ou illégales (voir *Introduction*).

Or, au niveau stratégique, il paraît préférable d'appréhender l'ensemble du spectre de la menace comme un *continuum* cohérent d'opérations considérées à l'aune de leur finalité commune d'influence malveillante à l'égard de la France, que celles-ci soient transparentes ou dissimulées, de la diplomatie publique agressive jusqu'aux actions d'ingérences informationnelles caractérisées, pour présenter un éventail des mesures de protection ou de riposte gradué en conséquence.

La référence à la notion d'influence paraît enfin de nature à faciliter l'intégration et l'articulation, au sein d'une même stratégie, non seulement des dispositifs de protection face aux ingérences étrangères à finalité d'influence sur le territoire national ainsi qu'un ensemble de politiques publiques sectorielles et d'actions visant à renforcer la résilience de la société face à celles-ci, mais également la structuration d'une aptitude interarmées relative à l'influence et la lutte informationnelle ainsi que des politiques d'influence affirmative de nature diplomatique. L'ensemble de ces enjeux de politique publique, en effet, sont reliés par un même objectif stratégique de nos compétiteurs, celui d'affaiblir notre pays par la voie de l'influence malveillante.

Il n'en va naturellement pas de même dans le cadre d'une action de niveau législatif, qui n'est fondée à viser que des comportements illicites ou dissimulés, comme le fait la récente loi visant à prévenir les ingérences étrangères en France.

Cette stratégie devra enfin comporter une dimension prospective, et s'intéresser aux évolutions prévisibles de la menace liée aux influences étrangères, notamment à l'aune du développement des technologies d'intelligence artificielle.

c) Une architecture par « cercles concentriques »

Cette stratégie étant globale, nationale et interministérielle devra nécessairement être ordonnée.

La commission d'enquête propose pour se faire de retenir une approche « par cercles concentriques », en distinguant trois groupes cohérents d'actions, selon une logique similaire à celle appliquée en Australie (voir encadré *supra*).

Le premier cercle concerne l'action régaliennne. Il comprend à cet égard les actions ayant trait à :

- la prévention, la détection et la riposte aux ingérences étrangères à finalité d'influence sur le territoire national (SGDSN, Viginum, DGSI, police, gendarmerie, DACG) ;

- la lutte contre les influences malveillantes et le développement d'une politique d'influence affirmative dans le champ diplomatique (ministère des affaires étrangères)

- l'aptitude des armées à la guerre d'influence et la lutte informationnelle (pôle ASO de l'état-major des armées, Comcyber, délégation à l'information et à la communication de la défense - Dicod) ;

- au renseignement (DGSI, DGSE, Tracfin) ;

- la sécurité économique, considérée sous l'angle de l'influence (Sisse).

S'agissant de ces actions, il va de soi que la version publique de la stratégie pourra être expurgée d'éléments ayant vocation à faire l'objet d'une diffusion restreinte voire d'une classification.

Le deuxième cercle concerne les politiques publiques sectorielles. Il comprend à cet égard l'action des ministères et agences concourant directement ou indirectement à la résilience de la nation face aux influences étrangères malveillantes, soit notamment les politiques publiques relatives :

- la régulation des médias et des plateformes numériques (Direction générale des médias et des industries culturelles - DGMIC, Arcom) ;

- le contrôle de la vie publique et politique (Haute autorité pour la transparence de la vie publique - HATVP - et Commission nationale des comptes de campagne et des financements politiques - CNCCFP) ;

- la protection des universités et de la recherche (Haut fonctionnaire de défense et de sécurité - HFDS - des ministères de l'éducation nationale, de la jeunesse et des sports, ou encore de l'enseignement supérieur et de la recherche) ;

- à la régulation de la vie associative.

Enfin, le troisième cercle concerne une série d'actions menées en direction et en collaboration avec la société civile, soit :

- pour sensibiliser à la menace l'ensemble des pans de la société, en incluant les acteurs publics (collectivités territoriales) que les corps intermédiaires (syndicats) ou encore que les acteurs privés (médias, associations, organisations non gouvernementales, entreprises...) ;

- pour renforcer par tout moyen la résilience de la population et bâtir une société où chacun se considère comme pleinement acteur de sa protection et de celle des autres.

d) L'importance d'intégrer d'emblée les enjeux de financement

L'exercice consistant à donner un chiffrage global des moyens budgétaires nécessaires à la mise en œuvre de cette stratégie serait délicat, sinon artificiel. Celle-ci combinerait en effet le fléchage de moyens existants,

le cas échéant réorientés, et le renforcement de certaines lignes budgétaires à un niveau qui devra être affiné en tenant compte des besoins nouveaux liés à l'aggravation de la menace. Un tel renforcement supposerait inévitablement, eu égard à la situation dégradée des finances publiques, des choix politiques et une réévaluation de la hiérarchie de nos priorités.

À ce stade, et sans chercher à se prononcer de façon ferme sur les moyens à mobiliser, la commission d'enquête considère de poser comme principe que la stratégie devra se donner pour exigence d'intégrer, pour chacun de ses éléments, l'enjeu des moyens qui leur seront consacrés et de leur financement.

Il y va, en effet, de l'efficacité, de la crédibilité et de la lisibilité pour le citoyen de cette stratégie.

À titre d'exemple, la Stratégie nationale d'influence élaborée par le ministère de l'Europe et des affaires étrangères ne fait aucune mention des moyens qui seront consacrés à sa mise en œuvre.

Pourtant, comme l'a clairement exposé le professeur Frédéric Charillon lors de son audition : « *l'influence suppose des moyens. On ne peut prétendre avoir une stratégie d'influence, à moyens constants, formule que nous aimons particulièrement en Europe. L'influence a un coût. Les pays qui ont mis en place des stratégies d'influence ont choisi d'y consacrer des moyens financiers, et ont opté pour cette priorité plutôt que d'autres, au titre de leur action extérieure. Il faut bien garder à l'esprit que si on accepte cette définition de l'influence qui est de se donner les moyens de faire changer le comportement des acteurs tiers, alors cette politique a un coût, sauf à considérer que nous sommes, par notre seul discours, absolument géniaux et que la brillance de ce discours suffira à rallier à nous toutes les bonnes volontés du monde. Personnellement, j'en doute* »¹.

Autre exemple : les auditions conduites par le rapporteur ont permis de mettre en évidence la difficulté, pour certains établissements d'enseignement supérieur et de recherche, de mettre en place les zones à régime restrictif (ZRR) compte tenu des coûts de sécurisation qu'ils représentent. Ce cas illustre bien les limites d'une politique de protection qui n'intègre pas d'emblée les enjeux de financement.

e) La nécessité d'associer le Parlement

Au plan de la méthode, l'élaboration d'une telle stratégie pourrait être confiée à un ou plusieurs groupes de travail interministériels pilotés par le SGDSN.

Cependant, la commission d'enquête considère que, s'agissant d'une problématique qui engage la nation dans son ensemble, et d'une politique animée par la volonté de bâtir, à long terme, une société dans laquelle chacun serait acteur de sa propre protection et de celle des autres face aux influences étrangères malveillantes, cette stratégie ne saurait être élaborée uniquement

¹ [Audition](#) du 29 février 2024.

« en chambre », dans le secret des bureaux comme ce fut le cas pour la revue nationale stratégique 2022.

Une association de la représentation nationale serait ainsi nécessaire pour asseoir la pleine légitimité de cette stratégie. En tout état de cause, dans la mesure où sa mise en œuvre n'est susceptible de concerter que marginalement le domaine de la loi, ce serait pour lui la seule occasion de se prononcer clairement sur cette problématique majeure de politique publique.

La définition de la stratégie pourrait ainsi donner lieu, à plusieurs étapes de son élaboration, à des auditions devant les commissions compétentes des deux assemblées de façon à créer les conditions d'un réel débat avec les parlementaires sur ses orientations, objectifs, et actions.

Une fois finalisé, la stratégie pourrait ensuite faire l'objet d'une déclaration du Gouvernement devant chaque assemblée donnant lieu à un débat puis un vote, selon la procédure prévue à l'article 50-1 de la Constitution. Ce débat pourrait ensuite être organisé de façon annuelle, et permettre de dresser un état des lieux de la mise en œuvre de cette stratégie.

Recommandation n° 2 : Élaborer une stratégie globale, nationale et interministérielle de lutte contre les influences étrangères malveillantes, en intégrant d'emblée les enjeux de financement et en associant le Parlement. Un débat sur sa mise œuvre se tiendrait annuellement au sein des assemblées.

3. Mettre en place une gouvernance adaptée

a) Premier cercle : renforcer la coordination de l'action régaliennne, dans le respect des prérogatives de chacun

(1) Se doter d'une doctrine commune en matière de réponse

La meilleure coordination de l'action régaliennne en réponse aux opérations d'influence étrangères malveillantes suppose l'établissement d'une doctrine commune de réponse.

En premier lieu, face à une opération d'influence, il s'agit en effet d'établir, **premièrement, si celle-ci appelle une réponse ou si, pour éviter tout « effet Streisand », il convient au contraire d'ignorer l'attaque**, tout en restant vigilant. La détermination de critères objectifs, quantitatifs ou qualitatifs, pourrait être effectuée pour apprécier le niveau de gravité de l'attaque et, partant, la nécessité d'y répondre. Elle s'appuierait en particulier sur les études conduites en matière de réception des opérations d'influence

par les populations, que la commission d'enquête appelle de ses vœux (voir *recommandation n° 1*).

Il ne s'agirait pas, bien entendu, de conférer un caractère contraignant à ces critères, l'opportunité d'une réponse étant *in fine*, en tout état de cause, appréciée par l'autorité politique.

En second lieu, il s'agit de définir la mesure de riposte adéquate : divulgation, attribution, mesures diplomatiques, poursuites pénales etc. (voir *Deuxième partie, II*), et l'autorité compétente pour la porter.

D'après les documents internes du SGDSN auxquels la commission d'enquête a pu accéder, un groupe de travail aurait été institué dans le cadre du Colmi pour établir une telle doctrine de réponse, et devait rendre ses conclusions au printemps. Les mêmes documents montrent que ces travaux n'ont pas encore donné lieu à une restitution.

En tout état de cause, la définition d'une telle doctrine intégrant la question de l'impact des opérations d'influence dans la population doit se traduire, au plan organisationnel, par une association continue entre le Colmi et la TF2I, afin que le premier puisse, le cas échéant, éclairer la seconde sur l'ampleur d'opérations des opérations menées sur le territoire national aux fins de déterminer si une réponse diplomatique doit être envisagée.

La commission d'enquête souhaite insister sur l'importance d'établir à brève échéance cette doctrine, qui est de nature à renforcer considérablement la coordination de l'action des ministères régaliens.

Recommandation n° 3 : Établir une doctrine claire en matière de réponse aux opérations d'influence malveillantes.

(2) Dans le respect des compétences de chacun, conforter Viginum dans son rôle de chef-de-file de la lutte contre les ingérences ciblant l'espace numérique national

La commission d'enquête considère qu'après seulement trois ans d'existence, Viginum a fait la preuve de son utilité et son action est saluée par l'ensemble de ses partenaires institutionnels nationaux et internationaux. À ce titre, son modèle mérite d'être pleinement conforté.

Cela implique de veiller à ce que chaque structure exerçant des activités de veille en source ouverte en matière d'opérations d'influence malveillantes conduites dans l'espace numérique s'en tienne à son champ de compétence, qui découle des principes fondamentaux de notre organisation institutionnelle en matière de défense et de sécurité nationale, expressément rappelés dans le code de la défense (voir *encadré*).

Les dispositions du code de la défense relatives à la répartition des compétences en matière de défense et de sécurité nationale

Article L. 1142-1 - Le ministre de la défense est responsable de la préparation et de la mise en œuvre de la politique de défense. Il est en particulier chargé de l'infrastructure militaire comme de l'organisation, de la gestion, de la mise en condition d'emploi et de la mobilisation des forces armées et des formations rattachées (...)

Article L. 1142-2 - Le ministre de l'intérieur est responsable de la préparation et de l'exécution des politiques de sécurité intérieure et de sécurité civile qui concourent à la défense et à la sécurité nationale et il est, à ce titre, sur le territoire de la République, responsable de l'ordre public, de la protection des personnes et des biens ainsi que de la sauvegarde des installations et ressources d'intérêt général (...)

Article L. 1142-3 - Le ministre chargé de l'économie est responsable de la préparation et de l'exécution de la politique de sécurité économique. Il prend les mesures de sa compétence garantissant la continuité de l'activité économique en cas de crise majeure et assure la protection des intérêts économiques de la Nation (...)

Article L. 1142-6 - Le ministre des affaires étrangères traduit, dans l'action diplomatique au niveau européen et au niveau international, les priorités de la stratégie de sécurité nationale et de la politique de défense (...)

Article L. 1142-7 - Le ministre de la justice assure en toutes circonstances la continuité de l'activité pénale ainsi que l'exécution des peines (...).

Source : code de la défense

À ce titre, la commission d'enquête ne peut que souscrire aux propos tenus par le ministre des armées Sébastien Lecornu, lors de son audition par la commission d'enquête : « *il peut exister des redondances, des phénomènes d'anthropophagie entre les services pour attirer les meilleurs talents, etc. Mais l'essentiel est de veiller attentivement à ce que l'abolition des frontières par le numérique ne remette pas en cause les grands équilibres issus de la Constitution de 1958 quant à la répartition des rôles entre les différents ministères sur les sujets de sécurité* ».

Dans ce contexte, il convient de relever que seul Viginum dispose du mandat de protéger le débat public numérique français. Toute confusion des périmètres ou redondance des moyens sur cette finalité précise serait ainsi préjudiciable pour la protection des intérêts fondamentaux de la Nation.

Il convient de s'assurer que chaque entité reste donc bien dans son périmètre, soit, pour rappel :

- les ingérences numériques étrangères pour Viginum ;
- les atteintes à l'image de la France à l'étranger pour la DCP du Quai d'Orsay ;
- la lutte d'influence menée contre les forces engagées sur des théâtres extérieurs et les atteintes à la politique de communication des armées, respectivement pour le Comcyber et la Dicod du ministère des armées.

Les instances interministérielles (Colmi et TF2I) doivent à ce titre continuer de jouer leur rôle de coordination, eu égard aux liens naturels qui peuvent être constatés entre ces différents types d'opérations ainsi que trancher d'éventuels conflits de compétence, sous l'autorité du SGDSN.

La consécration de Viginum en tant que protecteur du débat public numérique français passe, pour la commission d'enquête, par un renforcement de son modèle.

Ce modèle se caractérise actuellement par deux éléments centraux :

- un positionnement interministériel, en tant que service du SGDSN ;

- une approche fondée sur la seule révélation de manipulations de l'information dans le débat public numérique national, manifestées par des comportements inauthentiques sur les plateformes numériques, et en aucun cas sur la vérification de la manipulation de l'information, afin de ne pas se voir reprocher d'agir comme un « ministère de la vérité » ;

- la mise en place, en son sein, d'un comité éthique et scientifique, notamment au titre de l'activité de traitement de données personnelles de Viginum (voir encadré *infra*).

Ces deux derniers éléments garantissent la crédibilité de Viginum auprès de la société civile, et notamment des médias.

DOCUMENT PROVISOIRE

Le comité éthique et scientifique de Viginum

Placé auprès du secrétaire général de la défense et de la sécurité nationale, le comité éthique et scientifique de Viginum a pour mission de suivre l'activité du service. Il est le garant de son bon fonctionnement. Ses membres incluent des personnalités qualifiées dans les domaines juridictionnels, diplomatiques, scientifiques ou médiatiques.

Depuis le 3 novembre 2023, le comité éthique et scientifique est présidé par M. Jean-Luc Sauron, conseiller d'État. Il est composé de :

- M. Benoît Loutrel, membre du collège de l'Arcom ;
- M. Claude Kirchner, Directeur de recherche émérite de l'Institut national de recherche en sciences et technologies du numérique (Inria) ;
- M. Aymeril Hoang, Expert en numérique ;
- Mme Camille Malplat, journaliste à l'AFP, coordinatrice de la cellule investigation numérique pour l'Afrique francophone ;
- Mme Isabelle Mandraud, journaliste au Monde ;
- M. Jérôme Marilly, magistrat, adjoint au général, commandant du commandement du ministère de l'intérieur dans le cyberspace (Comcyber-MI) ;
- Jean-Maurice Ripert, Ambassadeur de France.

Le comité éthique et scientifique est destinataire de toutes les productions opérationnelles de Viginum. Il est systématiquement informé de l'ouverture et de la clôture des opérations menées par le service et reçoit les informations relatives aux déclenchements et à la durée des collectes automatiques de données à caractère personnel.

Le comité peut adresser à Viginum des recommandations sur les conditions d'exercice des missions du service. Enfin, il établit un rapport annuel, rendu public, que son président adresse au Premier ministre.

Source : Viginum, réponses au questionnaire du rapporteur

À cet égard, la commission d'enquête préconise **de faire de Viginum une véritable agence de l'État**¹ dotée de la personnalité morale et donc d'une autonomie de gestion accrue tout en préservant une tutelle juridique du SGDSN.

Une telle autonomie, notamment budgétaire, est de nature à accompagner la montée en puissance et la lisibilité de la politique publique portée par Viginum, conformément aux préconisations de la commission d'enquête (voir *infra, II*).

Dans ce cadre, le comité éthique et scientifique actuel pourrait, dans le cadre de ce changement de statut, évoluer en comité de pilotage éthique et

¹ Le Conseil d'État donne une définition de l'agence de l'État dans son [rapport annuel de 2012 « Les agences : une nouvelle gestion publique »](#). Celle-ci est fondée sur deux éléments : l'autonomie, et l'exercice d'une responsabilité qualifiée de « structurante » dans la mise en œuvre d'une politique nationale. Il est à noter que la notion d'autonomie est à distinguer de la notion d'indépendance.

scientifique qui serait placé auprès du conseil d'administration de l'agence, afin de se prononcer sur les conditions d'exercice de l'activité, et de fournir des réflexions indépendantes sur ses orientations stratégiques, sans préjudice des prérogatives de l'autorité de tutelle.

Le maintien d'une tutelle du SGDSN reste indispensable, l'activité de Viginum étant indissociable de la politique de sécurité nationale, dont la conduite ne saurait se soustraire à l'autorité politique. Ainsi, Viginum ne devrait en aucun cas se voir doter le statut d'autorité indépendante.

Conforter Viginum comme chef-de-file de la protection du débat public numérique lui permettrait de renforcer son rôle d'animation du Colmi. En particulier, Viginum pourrait proposer au SGDSN, en fonction des sujets à aborder, à en élargir ponctuellement la composition pour y accueillir des acteurs habilités pertinents, tels que des hauts fonctionnaires de défense et de sécurité (en particulier celui du ministère de l'enseignement supérieur et de la recherche) ou encore le Sisse du ministère de l'Économie et des finances, dans une perspective de meilleure articulation entre les politiques de lutte contre les influences étrangères malveillantes et sécurité économique (voir *infra, II et IV*).

Des relations plus structurées pourraient notamment être établies avec les équipes de veille en source ouverte :

- de la Dicod du ministère des armées, dans la mesure où certains sujets sur lesquelles elle exerce sa veille peut recouper l'enjeu de protection du débat public national. À titre d'exemple, les campagnes de désinformation concernant le soutien de la France à l'Ukraine (voir *Deuxième partie, II, B*) constituent à la fois une entrave à la politique de communication des armées et une ingérence dans le débat public français ;

- du secrétariat général du comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR), au titre de la veille sur les opérations d'influences d'inspiration islamiste sur les réseaux sociaux, dès lors que celles-ci émanent d'acteurs étrangers.

À cet égard en effet, seul Viginum dispose d'une habilitation réglementaire pour opérer un traitement de données de nature à caractériser finement l'opération d'ingérence.

Recommandation n° 4 : Conforter Viginum dans son rôle de chef-de-file en matière de protection du débat public numérique, en lui conférant un statut d'agence de l'État dotée d'une autonomie de gestion et placée sous la tutelle du secrétariat général de la défense et de la sécurité nationale (SGDSN).

b) Deuxième cercle : renforcer le pilotage interministériel et intra-ministériel

La stratégie nationale et interministérielle de lutte contre les influences étrangères malveillantes que la commission d'enquête appelle de ses vœux doit couvrir l'ensemble des politiques publiques sectorielles concernées par la menace.

À ce titre, les auditions menées par la commission d'enquête ont clairement mis en évidence le fait que, si les ministères régaliens s'étaient pleinement outillés pour y répondre, conformément à leur vocation, les autres ministères concernés par cette menace ne se sont emparés de ces enjeux de façon variable, même si des progrès considérables ont été réalisés au cours des dernières années.

Des points de contacts entre la sphère régaliennes et les ministères sectoriels et autorités de régulation concernées existent, mais ont été institués de façon très empirique. On peut citer notamment à la mise en place de divers groupes de travail interministériels mis en place par le SGDSN pour réaliser une veille et une analyse des risques liées aux influences étrangères, notamment dans le domaine de la recherche, pris en exemple lors de l'audition de la ministre de l'enseignement supérieur et de la recherche, Sylvie Retailleau¹.

Par ailleurs, au-delà de l'enjeu de la coordination horizontale interministérielle, qui s'effectue au niveau des ministres ou des directions centrales, se pose également la question de la façon avec laquelle les exigences liées à la protection contre les influences étrangères malveillantes sont ensuite diffusées aux niveaux intra-ministériel et à l'échelon déconcentré. Dans le domaine de l'enseignement supérieur et de la recherche, l'absence de mise en place, au niveau national, de lignes directrices claires en matière de procédure de détections des influences étrangères au sein des établissements, rappelé supra (voir *Deuxième partie, III, C*) en constitue l'illustration.

La commission d'enquête fait sien le constat posé à cet égard par le ministre des armées, **Sébastien Lecornu** lors de son audition, qui vaut tant pour la sécurité informationnelle que pour la cybersécurité : « *je trouve que la dynamique horizontale, c'est-à-dire l'interministérialité, fonctionne bien, notamment grâce au SGDSN, voulu par le général de Gaulle (...). En cas d'incident, une espèce de task force s'organise et tout le monde se met autour de la table (...). En revanche, dans certains ministères, la verticalité laisse à désirer. Si vous avez des ministres, des cabinets ministériels, des directeurs d'administration centrale, qui considèrent au fond que ce n'est pas leur boulot, car c'est celui du ministère de l'intérieur et du ministère des armées, et que l'information ne redescend pas - au hasard dans chaque agence régionale de santé (ARS) ou dans chaque*

¹ [Audition](#) du 18 juin 2024.

rectorat -, on n'y arrivera pas. C'est donc plus un problème de verticalité que d'horizontalité »¹.

Enfin, la stratégie interministérielle et la gouvernance mise en place pour son application doit se donner pour objectif de **diffuser, au sein de l'ensemble des administrations, dans les trois fonctions publiques, une culture de la protection face aux influences étrangères malveillantes**. Cette problématique a vocation à être prise en compte de façon constante et être intégrée d'emblée à l'ensemble des dispositifs, dès lors qu'ils sont rattachables à un secteur potentiellement concerné par la menace.

S'agissant par exemple de l'éducation nationale : si les dispositifs spécifiques d'éducation aux médias et à l'information ont naturellement leur rôle à jouer, la meilleure solution, pour œuvrer efficacement à la résilience de la nation face aux opérations d'influences étrangères malveillantes, reste d'intégrer cette problématique de façon transversales et diffuse dans les enseignements. Lors de son audition, l'Ambassadeur pour le numérique Henri Verdier pouvait ainsi souligner que « *certains pays ont fait des choses remarquables dans ce domaine, comme la Finlande. Son système éducatif intègre ces problématiques dans chaque matière : en mathématiques, on explique la manipulation des statistiques ; en histoire de l'art, on montre comment un changement de cadrage peut changer le sens d'une photo ; en histoire, on étudie la rhétorique fasciste et bolchevique, etc. Chaque professeur contribue à ce qui est plus une éducation des enfants pour en faire des citoyens armés intellectuellement qu'une simple sensibilisation à la désinformation* »². Cette conception contraste fortement avec le dispositif français actuel d'éducation aux médias et à l'information, qui ignore largement ces problématiques (voir *Deuxième partie, III*).

Une telle conception du rôle de chaque administration rejoint l'idée structurante de l'approche proposée par la commission d'enquête, selon laquelle la lutte contre les influences étrangères malveillantes est l'affaire de tous.

Pour impulser cette nouvelle culture, un portage politique fort est indispensable, à l'instar de ce qui se pratique en Australie avec la désignation, depuis 2018 d'un coordinateur national de la contre-ingérence (voir encadré *supra*).

Le travail mené par le SGDSN est louable, mais rencontre une limite inhérente à la nature administrative de cet acteur.

À ce titre, la commission d'enquête souscrit pleinement à l'analyse formulée lors de son audition par secrétaire général de la défense et de la sécurité nationale lui-même, le Préfet Stéphane Bouillon : « *en tant que fonctionnaire, je rends des comptes, notamment devant vous, mais n'étant pas un homme politique, je ne suis pas responsable devant vous comme l'est un membre du Gouvernement ; puisque je suis au service du Premier ministre, c'est lui qui est*

¹ [Audition](#) du 25 juin 2024.

² [Audition](#) du 25 mars 2024.

responsable devant vous de mes actes. À un moment ou à un autre, il conviendra de se demander dans quelle mesure cette mission [de pilotage interministériel de la politique de lutte contre les influences étrangères] ne devrait pas échoir à un secrétaire d'État ou à un ministre, qui assumerait une responsabilité globale, et non pas au titre, comme moi, du code de la fonction publique ou du code de la défense. (...) Compte tenu de l'ampleur et de la sensibilité du sujet, dans un grand pays comme le nôtre, il appartient au Gouvernement de s'en emparer »¹.

Ainsi, la commission d'enquête préconise de réaffirmer le portage politique par le Premier ministre de la politique de lutte contre les influences étrangères malveillantes en la confortant par la désignation d'un membre du Gouvernement dédié à cette matière, placé auprès de lui et qui pourrait à ce titre s'appuyer sur les services du SGDSN. Il serait chargé de garantir le bon fonctionnement de la coordination interministérielle et apporterait son concours aux autres ministères pour accompagner la mise en œuvre de la stratégie. Son action se déploierait également en direction des élus, de la société civile et des corps intermédiaires, dans le but de faire émerger une culture nationale de la protection face aux influences étrangères malveillantes

Il aurait notamment vocation à répondre devant le Parlement de l'action du Gouvernement le cadre des travaux de contrôle effectués en séance ou en commission ainsi que de représenter ce dernier pour l'examen de textes législatifs relatifs à la lutte contre les influences étrangères malveillantes. Le fait que, lors de l'examen en séance de la récente proposition de loi visant à lutter contre les ingérences étrangères, le Gouvernement ait été représenté devant les deux chambres par le ministre délégué chargé de l'Europe, sans que le texte ne présente de lien direct avec son portefeuille, illustre bien la problématique.

Recommandation n° 5 : Réaffirmer le portage politique par le Premier ministre de la politique de lutte contre les influences étrangères malveillantes en la confortant par la désignation d'un membre du Gouvernement placé auprès de lui qui en aurait la charge.

c) *Troisième cercle : « ne pas en faire trop » et organiser l'autodéfense de la société civile*

S'agissant d'une menace qui cible la société dans son ensemble, l'action des pouvoirs publics ne saurait être suffisante, à plus forte raison dans le contexte français.

¹ [Audition](#) du 11 juin 2024.

Cette conscience de la nécessité de confier, au moins en partie, à la société la responsabilité de sa propre résilience a bien été exprimée par la formule le Préfet Stéphane Bouillon, lors de son audition par la commission d'enquête, qu'il ne faut pas entendre comme un aveu d'impuissance mais bien comme une marque de confiance : « *je ne veux pas en faire trop* »¹.

Il précise : « *ce n'est pas à l'État de tout faire dans ce domaine. Je trouve que le rôle des « fact-checkers » des médias, qui vérifient les informations et leur provenance, est excellent et extrêmement sain pour la société, tout comme les enquêtes spécialisées des journaux (...) Certes, nous avons un rôle important à jouer, comme une tour de contrôle, mais cela vient en plus des actions plus générales de sensibilisation et d'éducation des différents acteurs*

Dans d'autres pays, bénéficiant d'un niveau de confiance dans les institutions plus solide que la France, l'État peut jouer un rôle fortement proactif dans la « *défense psychologique* » de la société civile, pour reprendre l'intitulé de l'agence exerçant cette mission dans le domaine en Suède (voir encadré) et qui constitue un modèle unique en matière de lutte contre les influences étrangères malveillantes. Outre des travaux de détection comparables à ceux conduits par Viginum, l'Agence de défense psychologique suédoise mène des actions de sensibilisation et de financer des projets de recherche et soutien les médias.

L'Agence de défense psychologique suédoise

Le principal organisme concerné par la lutte contre les influences étrangères est l'Agence de défense psychologique. Crée à la fin des années 1950 dans le contexte de la guerre froide, puis démantelée en 2008, elle a été rétablie en janvier 2022 dans le contexte de la réactivation du concept de « Défense totale », dont elle est l'incarnation la plus visible. Elle comprend environ 60 personnes, ainsi que 2 personnes à la représentation permanence de la Suède auprès de l'Union européenne, un personnel à Tallinn et un autre auprès de l'Otan.

Présentée comme un pont entre la défense militaire et la défense civile, la mission de l'Agence consiste à « *protéger la société ouverte et démocratique et la libre formation d'opinions en identifiant, analysant et répondant aux influences inappropriées et autres informations trompeuses dirigées contre la Suède ou les intérêts suédois* », à travers quatre fonctions :

1^o Générer une prise de conscience des tentatives d'influence de la part d'acteurs étrangers dont la société suédoise est l'objet. Ce travail de sensibilisation se traduit par des campagnes de communication (ex : « *Don't be fooled* »), ayant souvent recours à l'humour pour ne pas augmenter l'anxiété. L'agence s'appuie aussi sur des organisations de la société civile à même de relayer ces messages vers les populations défavorisées. À ce titre, l'agence effectue un travail de recherche sur l'évolution de la société civile, et constate notamment que les nouvelles formes d'activismes, plus éruptives et volatiles, constituent de fait des relais moins structurants que les traditionnelles organisations sociales (clubs, associations, etc.), qui ont tendance à s'affaiblir. Comprendre la société et ses codes permet de mieux appréhender pourquoi tel ou tel phénomène informationnel prend ou non, cela participe à la résilience. Par ailleurs, l'agence travaille avec les responsables de la sécurité du Parlement pour organiser des formations sur la base du volontariat ;

¹ [Audition](#) du 11 juin 2024.

2° Déetecter, et parfois dévoiler les campagnes de désinformation menées contre la Suède. L'agence peut aussi proposer au gouvernement des mesures offensives pour répondre à des attaques dans le champ informationnel. En Suède, la plupart des tentatives d'ingérence et de manipulation de l'information proviennent de Russie, mais aussi de Chine et d'Iran. L'agence serait notamment intéressée par l'action de la Russie en Afrique du Nord.

3° Financer des projets de recherche, par exemple sur la « *volonté de défendre le pays* ». Plusieurs études indiquent que 80 à 90% des Suédois seraient prêts à se mobiliser pour défendre le pays, dont environ la moitié en prenant les armes. L'agence travaille étroitement avec les instituts de recherche.

4° Soutenir les médias, en organisant des formations (en coopération avec les universités) ou en leur offrant une aide s'ils se retrouvent au cœur d'une campagne de déstabilisation. L'agence réunit ainsi régulièrement les rédacteurs en chef des médias suédois et des représentants des plateformes numériques, pour échanger sur le paysage informationnel et les menaces observées.

Face aux attaques hybrides, les responsables de l'Agence de défense psychologique mettent en avant leurs réussites après deux ans d'existence : le travail de sensibilisation auprès de la société civile sur les opérations d'influence étrangère et une crédibilité acquise auprès du gouvernement, qui peut s'appuyer sur cette agence en cas d'attaques informationnelle. Ce modèle d'agence fonctionne en Suède grâce à la forte confiance de la population envers les autorités et les principaux médias (auprès desquelles l'agence effectue un travail de sensibilisation).

Source : commission d'enquête, d'après les réponses de l'Ambassade de France en Suède au questionnaire du rapporteur

En France, où le niveau de confiance dans les institutions et les discours officiels est plus faibles, il paraît judicieux pour l'État de se mettre quelque peu en retrait et de se limiter à accompagner la société dans l'organisation de sa propre autodéfense.

À cette fin, la commission d'enquête préconise de s'inspirer, tout en l'élargissant, de la recommandation du rapport de la mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences¹ tendant à la création d'un « *observatoire des influences étrangères et de leurs incidences sur l'enseignement supérieur et la recherche* » qui associerait universitaires, ministères de l'enseignement supérieur et de la recherche, des affaires étrangères, de l'économie, de l'intérieur et des armées, chargé de dresser un état des lieux, d'en assurer le suivi régulier et de formuler des propositions au Gouvernement.

Pourrait ainsi être institué, plus largement, un **observatoire des influences étrangères malveillantes** regroupant les parties prenantes de la société civile : chercheurs, médias (en particulier les équipes de vérification des faits *etc.*), tout en associant les acteurs publics concernés, notamment

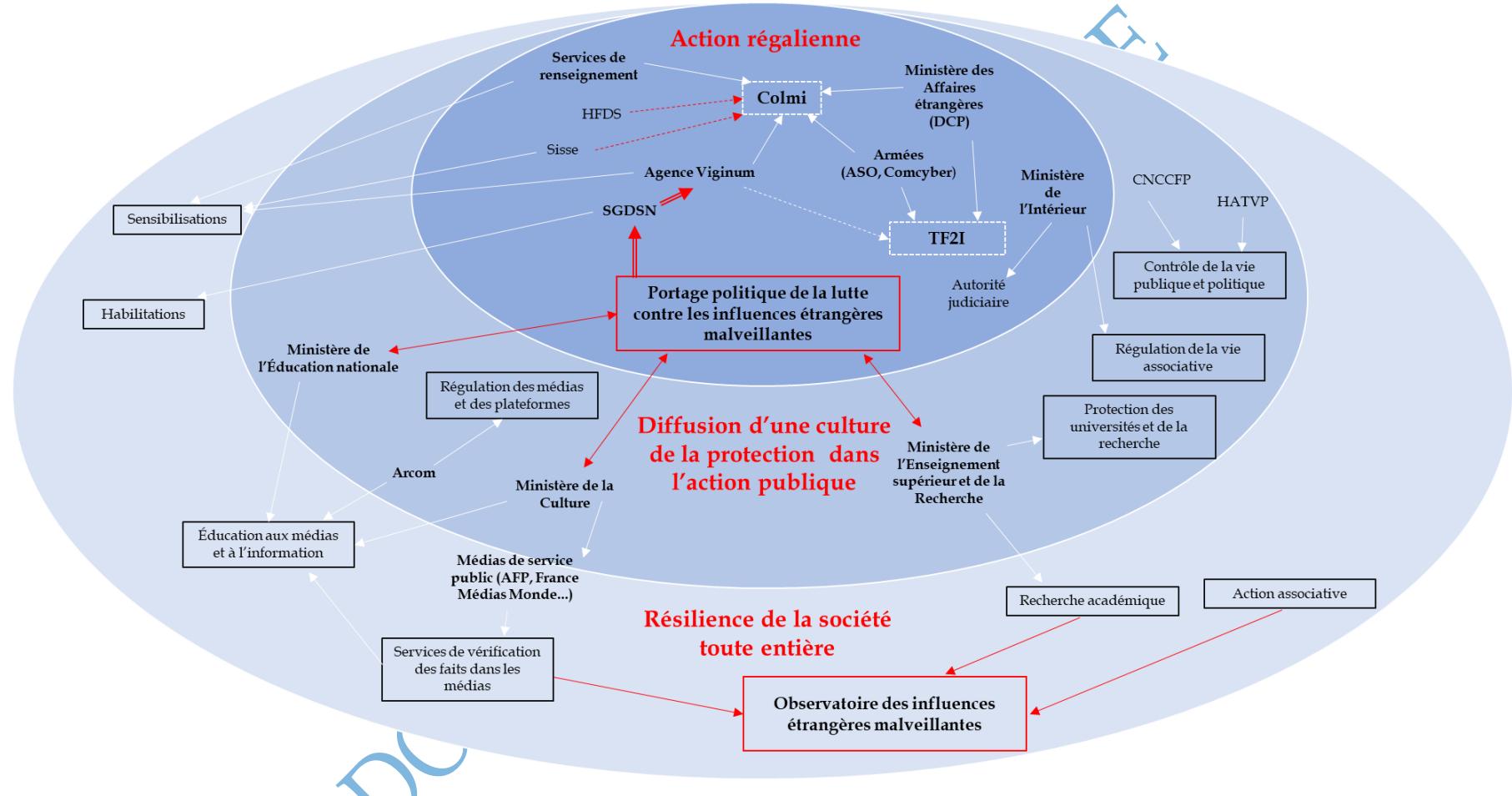
¹ [Rapport d'information n° 873 \(2020-2021\)](#) fait par André Gattolin au nom de la mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences, déposé le 29 septembre 2021.

Viginum. Il s'agirait d'une instance de partage et de mise à jour de connaissances (en particulier les résultats de la recherche), de bonnes pratiques, et de propositions, dont le fonctionnement serait totalement indépendant du Gouvernement.

Recommandation n° 6 : Mettre en place un observatoire des influences étrangères malveillantes regroupant les parties prenantes de la société civile et les acteurs publics concernés.

DOCUMENT PROVISOIRE

Architecture de la stratégie de lutte contre les influences étrangères malveillantes proposée par la commission d'enquête



Légende : cadre pointillé : instance de coordination ; cadre noir : actions ; flèche : lien, flèche en pointillés : lien possible ; flèche double : autorité ou tutelle ; en rouge : proposé par la commission d'enquête par la commission d'enquête.

Source : commission d'enquête

II. PREMIER CERCLE : LES MINISTÈRES RÉGALIENS, « NOYAU DUR » DE LA RÉPONSE AUX OPÉRATIONS D'INFLUENCES ÉTRANGÈRES

A. LUTTER CONTRE LES INFLUENCES ÉTRANGÈRES SUR LE TERRITOIRE NATIONAL

1. Renforcer les dispositifs de veille et d'alerte

a) Adapter les moyens de Viginum à sa nouvelle fonction chef de file de la détection des manipulations de l'information

Dans le prolongement de l'objectif de doter Viginum d'une mission de chef de file de la fonction de sécurité informationnelle et d'un statut d'agence, il apparaît nécessaire d'aligner ses moyens matériels et juridiques sur ce nouveau cadre.

En premier lieu, sur le plan matériel, **les moyens affectés à la détection et la caractérisation des ingérences devraient être mis en adéquation avec les ambitions affichées** en termes de lutte contre les manœuvres informationnelles. L'état de la menace impose ainsi en particulier de renforcer les moyens humains de Viginum, faute de quoi ce service serait voué à demeurer une simple vitrine de la lutte contre les influences malveillantes.

En l'état actuel de ses effectifs, **Viginum est en mesure, comme exposé supra, de mener simultanément cinq « opérations permanentes »** : quatre opérations spécialisées selon des critères géographiques et linguistiques et une opération transversale sur les intérêts économiques, industriels et scientifiques français. **À ces opérations permanentes s'ajoutent des opérations ponctuelles portant sur des évènements spécifiques ou électoraux.**

Pour conduire ces actions de concert, le service devrait être doté de 58 équivalents temps plein (ETP) d'ici à la fin de l'année 2024, dont une quarantaine affectée aux opérations. Viginum ambitionne **d'augmenter ses effectifs à 95 ETP d'ici à 2027, avec un taux d'agents dédiés aux opérations de l'ordre de 70 %**. Cet effectif marque un net recul par rapport à la cible 2024 qui avait été fixée en 2021, et qui s'établissait à 65 ETP.

La commission d'enquête estime que ces moyens ne sont pas alignés sur les ambitions formulées pour ce service. Il importe de souligner que l'Anssi, pendant de Viginum pour la cybersécurité, comprenait 634 agents en 2023. **Sans envisager de porter les moyens de Viginum à un niveau équivalent à court terme, la commission d'enquête considère qu'il appartient de placer le schéma d'emplois de ce service en cohérence avec son mandat.** Pour rappel, les « *Kremlin Leaks* », un ensemble de documents internes à l'administration présidentielle russe révélés par un consortium de journalistes en 2024, ont permis de déterminer que la Russie **consacrait un**

budget de 1,1 milliard d'euros à la guerre informationnelle, en interne comme en externe.

Une hausse des effectifs de Viginum permettrait de répondre aux deux principaux défis auxquels le service devrait être confronté au cours des prochaines années.

D'une part, il devra être en mesure **d'élargir ses capacités opérationnelles pour compenser une intensification des campagnes de désinformation visant la France**. En particulier multiplication des manœuvres informationnelles agressives de la Russie, de la Chine et de l'Azerbaïdjan au cours des derniers mois démontre l'utilité du travail de veille. À ce titre, **Viginum indique un objectif, à terme, de huit opérations permanentes simultanées**. L'objectif qui doit être poursuivi est d'éviter un *scenario* dans lequel les capacités de détection et d'analyse seraient saturées face à une vague d'attaques simultanées, coordonnées ou non.

Parmi ces opérations, la commission d'enquête souligne **la nécessité d'intégrer une dimension prospective**. Dans le cadre d'une approche en trois piliers, exposée *supra*, il paraît indispensable de mieux appréhender l'impact des opérations d'influence. Dans le jeu « *du chat et de la souris* » que se livrent les services de détection et les responsables d'opérations d'influence, **la complexification des opérations et le développement de nouvelles techniques de manipulation et d'amplification adaptées aux spécificités de chaque réseau social** nécessite de la part de nos services une capacité de prospective. Pour ce faire, les opérations de Viginum devraient intégrer cette dimension d'anticipation en étant en mesure de déterminer les caractéristiques de diffusion propres à chaque plateforme et de classifier chaque mode opératoire.

Dans cette logique d'anticipation, Viginum entend se doter de nouvelles capacités internes au service qui reposeraient notamment sur un centre d'excellence en intelligence artificielle, issu de l'actuel « *datalab* » de Viginum. Les développements récents de l'intelligence artificielle **ont mis en exergue un risque de mobilisation, par des opérations d'influence malveillantes, de ces nouveaux outils**. La rapidité du perfectionnement de ces derniers doit conduire les services de détection à suivre de près ces évolutions. **Le centre d'excellence devra également permettre à Viginum de développer ses propres outils d'IA pour renforcer ses capacités de détection et de caractérisation.**

D'autre part, **les moyens alloués à la future agence Viginum devront également prendre en compte les nouvelles missions qui lui seront confiées**, au-delà de ses activités de détection et de caractérisation. En effet, Viginum a **exprimé à la commission d'enquête le souhait d'accroître sa participation au renforcement de la résilience de la société**, d'une part, et sa collaboration à la montée en puissance de services étrangers, d'autre part.

À ce titre, une « Académie de lutte contre les manipulations de l'information » devrait voir le jour au sein de Viginum. Cette structure permettrait de mettre au service de la société civile et de nos partenaires étrangers l'expérience accumulée par Viginum depuis sa création en 2021. L'Académie **pourrait ainsi développer des capacités de formation à destination de services alliés à l'étranger et d'acteurs intéressés de la société civile** (médias, vérificateurs d'information, entreprises, organisations non gouvernementales...). Elle constituerait ainsi un lien entre Viginum et la société civile, en assurant la publicité de ses travaux.

Ces nouveaux champs d'action, qui seront développés dans les parties *infra*, supposent d'y consacrer des moyens spécifiques, notamment en termes de profils recrutés. Dans un schéma d'emplois à 95 agents, **environ 20 % de ces effectifs seraient alors fléchés sur des activités de formation et de partenariats**. Il faudra néanmoins être vigilant, au sein de Viginum comme de son autorité de tutelle, le SGDSN, pour conserver une très large majorité des effectifs sur les fonctions opérationnelles de veille et d'analyse.

Recommandation n° 7: Conférer à Viginum des moyens humains et matériels en adéquation avec sa mission de chef de file en matière de protection du débat public numérique et identifier clairement, au sein des documents budgétaires et dans une logique de transparence, les crédits et les effectifs alloués.

En second lieu, sur le plan juridique, l'encadrement des opérations de Viginum par le décret n° 2021-922 du 13 juillet 2021¹ et celui n° 2021-1587 du 7 décembre 2021² pourrait être amené à évoluer. En effet, la mise en œuvre de ce cadre réglementaire par Viginum depuis 2021 a conduit le service identifier plusieurs pistes d'amélioration qui pourraient, selon la commission d'enquête, affiner ses capacités de détection et de caractérisation.

Premièrement, **limiter la collecte automatisée de contenus publiquement accessibles aux plateformes en ligne dont l'activité sur le territoire français ne dépasse pas cinq millions de visiteurs** par jour ne semble plus adaptée à la réalité des opérations de manipulation de l'information auxquelles est confronté Viginum. L'article 1^{er} du décret du 7 décembre 2021 mentionne en effet les « *plateformes en ligne des opérateurs*

¹ [Décret n° 2021-922 du 13 juillet 2021](#) portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères ».

² [Décret n° 2021-1587 du 7 décembre 2021](#) portant autorisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères.

mentionnés au I de l'article L. 111-7 du code de la consommation et dont l'activité sur le territoire français dépasse un seuil de cinq millions de visiteurs uniques par mois ». Une plateforme comme *LinkedIn* n'entre par exemple pas dans cette catégorie. Or Viginum a constaté que **certaines opérations pouvaient être menées sur des plateformes à plus faible audience mais dont les communautés d'utilisateurs sont très actives ou plus perméables** à la désinformation. De plus, les campagnes de manipulation de l'information en ligne peuvent se déployer simultanément sur plusieurs plateformes, combinant des plateformes en-dessous et au-dessus du seuil de cinq millions de visiteurs.

Deuxièmement, Viginum souhaiterait autoriser, dans le cadre de ses travaux de veille, la collecte automatisée de données. En l'état du droit, **la collecte automatisée n'est possible qu'à l'issue des travaux de veille et en application de critères techniques** permettant de délimiter le cadre de l'opération de détection et de caractérisation. Le décret du 7 décembre 2021 précise ainsi qu'« *aucune collecte automatisée de données à caractère personnel n'est mise en œuvre à l'occasion des travaux de veille* »¹. Dans la pratique, les actions de veille et de caractérisation s'opèrent en parallèle. Les « *critères techniques* », en principe déterminés à l'issue de la veille, sont modifiés en cours d'opération du fait de l'apport des données collectées.

Troisièmement, **une réflexion pourrait être engagée sur un allongement du délai maximal de renouvellement des collectes et du délai de conservation des données traitées**. Actuellement, l'article 2 du décret n° 2021-1587 du 7 décembre 2021 dispose que les données sont collectées « *pendant une période maximale de sept jours. Cette période peut être renouvelée, dans la limite d'une durée qui ne peut excéder six mois à compter du déclenchement de l'opération de collecte* ». Cette durée de collecte de six mois paraît toutefois relativement courte au regard de la durée des manœuvres surveillées. Le suivi des opérations *Portal Kombat* et *RRN* a démontré la résilience des réseaux de désinformation, impliquant un suivi dans le temps tandis que d'autres, comme *Olympyia*, ciblent des évènements plus de six mois en avance. En outre, à l'issue de leur exploitation, les données collectées sont détruites dans un délai de quatre mois.

Quatrièmement, la définition d'ingérence numérique étrangère (INE), prévue à l'article 1^{er} du décret du 13 juillet 2021, **pourrait utilement évoluer sur deux points : le caractère massif de la diffusion et les contenus objets de la diffusion**.

S'agissant du **caractère massif de la diffusion**, ce critère apparaît en pratique difficile à mettre en œuvre. Il n'existe, ni dans le décret du 13 juillet 2021 ni dans aucun autre texte, de définition précise du critère de la « massivité ». Son application **laisse place à une large marge d'appréciation pour le service**. La fixation d'un seuil à partir duquel cette condition serait remplie aurait pour inconvénient de poser arbitrairement une limite à la veille

¹ Article 2 du décret n° 2021-1587 du 7 décembre 2021.

de Viginum. Une suppression du caractère massif pourrait donc être envisagée.

Concernant la mention des contenus, la caractérisation d'une INE est conditionnée à ce que l'opération visée diffuse des « *allégations ou imputations de faits manifestement inexacts ou trompeuses* ». Sur un plan juridique, **le caractère manifestement inexact ou trompeur est d'une appréciation complexe, notamment pour un service administratif**. L'expertise de Viginum porte davantage sur les moyens techniques de diffusion que sur l'analyse sémantique des publications. Sur un plan pratique, **le critère d'une diffusion « artificielle ou automatisée » est plus pertinent** pour identifier une opération de manipulation de l'information en ligne. Cette dernière peut tout à fait porter sur une information véridique.

La commission d'enquête estime que ces évolutions potentielles de la définition de la notion d'INE sont positives. Viginum **ne doit pas devenir un « ministère de la vérité »**. Il importe, dans la lutte contre les influences malveillantes, de conserver comme boussole le respect de notre modèle démocratique. En s'abstenant de se prononcer sur la véracité des contenus diffusés de manière inauthentiques, **Viginum s'abstrait du débat politique pour demeurer uniquement dans un prisme technique**. Certes, une nouvelle définition d'INE allant dans le sens de ces recommandations irait dans le sens d'un élargissement de cette notion et par conséquent du contrôle de Viginum. Pour autant, **l'ingérence numérique étrangère ne constitue pas une infraction pénale et les activités de détection demeurent sous le contrôle d'un comité éthique et scientifique**. Par ailleurs, supprimer le critère du caractère trompeur ou inexact des contenus aurait pour effet de rapprocher la définition de l'INE de la notion de « *FIMI* » proposée par le Service européen pour l'action extérieure.

La commission d'enquête tient cependant à souligner que la préparation du n° 2021-1587 du 7 décembre 2021 découlait d'un travail de consultation poussé de la part du SGDSN, impliquant notamment des parlementaires. Une nouvelle rédaction de ce texte impliquera, par parallélisme des formes, une implication du Parlement.

Recommandation n° 8 : Renforcer les moyens juridiques de Viginum, en :

- Supprimant la référence au seuil des 5 millions de visiteurs uniques par mois pour les plateformes en ligne ;**
- Autorisant la collecte automatisée de données dans les activités de veille de Viginum ;**
- Allongeant le délai de conservation des données traitées et le délai de renouvellement des collectes ;**
- Revoyant la notion d'INE prévue par le décret du 13 juillet 2021 à l'aune de l'évolution de la menace et en précisant les conditions dans lesquelles Viginum peut mener ses investigations.**

b) Compléter les autres dispositifs de veille et d'alerte dans le domaine économique

Les opérations d'influence dans le domaine économique constituent un phénomène encore mal appréhendé par nos politiques publiques. L'action du Sisse, qui s'inscrit dans une logique de souveraineté économique, **vise en effet à protéger des entreprises jugées stratégiques de manœuvres capitalistiques**. De même, notre droit pénal, sans prévoir un cadre spécifique d'espionnage industriel, comporte des infractions qui permettent de caractériser ce type d'ingérences.

Pour autant, une action coordonnée, par un État hostile, d'investissements ciblés dans un secteur de notre économie ou un territoire spécifique échapperait aux **mécanismes de contrôle des investissements dès lors que les entreprises visées ne seraient pas incluses dans la liste des actifs stratégiques**. Pourtant, une entité étatique en mesure de contrôler une part très ciblée de l'activité économique d'un territoire disposerait d'un fort levier d'influence. À titre d'exemple, si un État hostile décida d'acquérir ou de soutenir financièrement l'ensemble des clubs de sport ou d'associations sportives sur un département, **il serait en capacité de diffuser un narratif auprès d'une part conséquente de la jeunesse locale et de potentiellement capter les élus ou responsables économiques de ce territoire**.

Il serait souhaitable de doter le Sisse, en lien avec les renseignements généraux, d'une mission de veille économique de manière à détecter **toute opération coordonnée d'investissement menée par un État ou une entité contrôlée par lui sur un territoire donné et dans un secteur non compris dans le champ des actifs stratégiques**. Cette nouvelle mission impliquerait

d'étoffer le réseau des délégués du Sisse placés auprès des préfets de région (les Disse).

À l'aune du développement de campagnes informationnelles d'influence visant des entreprises et des intérêts économiques français cette veille économique centrée sur les investissements devra s'articuler avec le travail de veille informationnelle mené par Viginum dans le cadre son opération permanente transversale.

Recommandation n° 9 : Se doter d'un outil de suivi des investissements étrangers en France à l'aune non plus seulement, comme le fait le Sisse, du caractère stratégique de leur objet mais de leur possible finalité d'influence à moyen-long terme.

2. Améliorer la judiciarisation des opérations d'influence malveillantes en mobilisant pleinement les dispositifs nouvellement adoptés

L'entrée en vigueur de la loi visant à prévenir les ingérences étrangères (loi « Ingérences étrangères ») **devrait permettre d'améliorer la judiciarisation des opérations d'ingérence à visée d'influence**, comme indiqué dans la deuxième partie du rapport. La création d'une circonstance aggravante applicable aux infractions contre les biens ou les personnes conduites dans le but de servir les intérêts d'une puissance étrangère ou d'une entreprise ou d'une organisation étrangère ou sous contrôle étranger devrait faciliter l'entraîne judiciaire à ce type d'opération. **La combinaison de ce dispositif avec l'autorisation des techniques spéciales d'enquête contribuera à accélérer la caractérisation des faits.**

Deux conditions sont toutefois nécessaires à une mise en œuvre effective des apports de la loi « Ingérences étrangères ».

D'une part, **il importe que ces nouvelles dispositions fassent l'objet d'une information pertinente auprès des juridictions**. La pluralité des juridictions potentiellement compétentes sur les infractions liées à des opérations d'ingérence implique, de la part de la direction générale des affaires criminelles et des grâces, **un travail de présentation et d'explication sur l'intégration de cette nouvelle circonstance aggravante dans le régime juridique applicable aux ingérences**. Le « Focus DACG » dédié, qui compile et commente l'ensemble des infractions mobilisables par l'autorité judiciaire, devra faire l'objet d'une mise à jour au plus vite après l'entrée en vigueur de la loi.

D'autre part, les échanges entre les services chargés de la veille et de la détection des opérations et les services du ministère de la justice devront être poursuivis et approfondis. Il s'agit, pour l'autorité judiciaire, de disposer des informations adéquates sur l'état de la menace, particulièrement évolutive au regard du contexte géopolitique et technologique, pour y répondre de manière appropriée. En miroir, il s'agit, pour les services de renseignement et le SGDSN, d'articuler les mesures judiciaires, dans l'arsenal des mesures d'entrave aux opérations d'influence.

Par ailleurs, la coopération renforcée entre Viginum et Pharos, dans le cadre de la convention bipartite de partenariat signée le 7 décembre 2023, devra prendre en compte la caractérisation de la nouvelle circonstance aggravante en cas d'ingérence étrangère créée par cette loi, dont le travail de qualification supposera une collaboration étroite entre les deux services.

Recommandation n° 10 : Mettre pleinement en œuvre le volet pénal de la loi « Ingérences étrangères », en diffusant largement aux magistrats l'information pertinente sur les nouveaux outils de lutte contre les ingérences étrangères et en intégrant pleinement la caractérisation de la nouvelle circonstance aggravante d'ingérence étrangère dans la coopération entre Pharos et Viginum. Intégrer cette dimension dans la formation des magistrats à l'École nationale de la magistrature.

B. DANS LE CHAMP DES ARMÉES, RÉÉVALUER LES MOYENS BUDGÉTAIRES À L'AUNE DES NOUVELLES MENACES

Si les armées et le Comcyber ont été les premiers à subir de manière prononcée la menace d'influence et ont, par conséquent, adapté leur doctrine et leurs opérations, les moyens dédiés à la lutte information d'influence (L2I) paraissent encore limités.

La loi n° 2023-703 du 1^{er} août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense (dite « LPM 2024-2030) avait pris en compte l'évolution du contexte stratégique et la montée des menaces hybrides. Pour cette raison, un effort particulier avait été consacré au renforcement des moyens du cyber et du renseignement, avec respectivement 4 et 5 milliards d'euros fléchés sur la période. Les deux domaines représentent également 27 % de l'augmentation nette des emplois du ministère des armées sur 2024-2030. Si l'effort porté sur le cyber comprenait une dimension de lutte informatique

d'influence, la problématique informationnelle n'a pas été spécifiquement identifiée.

Or, le contexte stratégique doit désormais inclure la récente montée des opérations d'influence agressives et la sophistication technologique croissante de ces actions. Les armées sont désormais **systématiquement visées par des manœuvres informationnelles et chaque déploiement des forces à l'étranger se trouve exposé à un risque réputationnel**. Compte tenu de ce contexte, l'état-major des armées note que **les capacités de veille et de détection paraissent aujourd'hui sous-dimensionnés**. Le développement de nouveaux outils technologiques de détection et d'analyse, en coopération avec la nouvelle agence ministérielle pour l'intelligence artificielle de défense¹, suppose également des moyens additionnels. Pour le général Bonnemaison, la montée en puissance des capacités de riposte « *suppose concrètement de mettre en place des dispositifs informationnels qui serviront de relais et permettront la saisie d'opportunités. Cela nécessite des moyens beaucoup plus importants que ceux dont je dispose, en potentialité de déploiement sur place, en capacités RH de détection, de caractérisation et de suivi* »².

Un rééquilibrage des crédits programmés en faveur de la lutte informationnelle serait par conséquent nécessaire. La LPM dispose, pour ce faire, que « *La présente programmation fera l'objet d'une actualisation par la loi avant la fin de l'année 2027. Précédée d'une actualisation de la revue nationale stratégique, cette actualisation permettra de vérifier l'adéquation entre les objectifs fixés dans la présente loi, les réalisations et les moyens alloués. Elle permettra également de consolider la trajectoire financière et l'évolution des effectifs en fonction des besoins mis à jour au regard de l'inflation, du contexte stratégique du moment et des avancées technologiques constatées* »³. À l'occasion de l'actualisation de la LPM d'ici à 2027, il serait donc opportun d'opérer une **ajustement des moyens dédiés** à la lutte informationnelle à l'aune de l'évolution rapide de la menace.

Recommandation n° 11 : Réévaluer, à l'occasion de la prochaine actualisation de la loi de programmation militaire, soit avant la fin de l'année 2027, les moyens de la lutte informationnelle à l'aune de l'évolution de la menace.

¹ Décret n° 2024-376 du 23 avril 2024 relatif au service à compétence nationale dénommé « agence ministérielle pour l'intelligence artificielle de défense ».

² [Audition](#) du 4 avril 2024.

³ Article 8 de la loi n° 2023-703 du 1^{er} août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense.

C. DÉVELOPPER NOTRE INFLUENCE POSITIVE À L'ÉTRANGER EN L'ARTICULANT À LA POLITIQUE DE LUTTE CONTRE LES INFLUENCES MALVEILLANTES

1. Chef de file de la fonction influence, le ministère de l'Europe et des affaires étrangères doit pouvoir disposer de moyens adéquats en matière de veille et de riposte

Le chef de filât de la « fonction influence » confié au ministère de l'Europe et des affaires étrangères **implique que ce dernier poursuive ses efforts de consolidation de ses moyens de communication et de riposte.**

À cet égard, lors de son audition devant la commission d'enquête, le ministre Stéphane Séjourné a indiqué que **la sous-direction « veille et stratégie » de la direction de la communication et de la presse pourrait se voir doter de compétences d'enquête en sources ouvertes.** Ce renforcement des moyens de détection et de caractérisation au sein du ministère est **cohérent avec la montée en puissance de la lutte contre les manœuvres informationnelles.** Il appartiendra néanmoins à la DCP de développer ces capacités dans le respect de la compétence de Viginum comme chef de file en matière de sécurité informationnelle. L'enquête en sources ouvertes représente en effet un savoir-faire largement développé au sein de Viginum. Il existe donc **un risque, en construisant des capacités similaires au sein d'un autre ministère, de dispersion des moyens** et de concurrence entre services.

Le renforcement des capacités de la sous-direction « veille et stratégie » devra donc respecter deux conditions pour être opérant et éviter une dispersion tubulaire de nos moyens de détection :

- d'une part, **assurer une coordination effective entre la sous-direction « veille et stratégie » et Viginum.** Pour ce faire, les instances de dialogue que constituent la TF2I et le Colmi pourront être mobilisées pour encourager ces synergies ;

- d'autre part, **intégrer dans ces capacités d'enquête une plus-value propre au ministère de l'Europe et des affaires étrangères**, à savoir l'analyse politique des opérations informationnelles et de leurs commanditaires.

À cet égard, cette expertise devrait permettre de renforcer, dans le cadre de la détection des opérations, l'anticipation des futures menaces. Le relais des postes diplomatiques et des directions géographiques constitue **un indispensable levier d'identification de l'émergence d'acteurs potentiellement hostiles.** Le basculement de nouveaux États dans des stratégies d'influence agressives, le cas azéri étant une illustration récente, pourra donc être mieux appréhendé.

En parallèle de ces capacités de détection, **il importe que le ministère poursuive ses efforts en faveur de la structuration d'une capacité de riposte, portée par la communication stratégique.** À ce titre, l'ouverture en juin 2024

d'un nouvel instrument de formation continue du personnel diplomatique, l'Académie diplomatique et consulaire (ADC), devrait contribuer à renforcer la professionnalisation des services de presse au sein des postes.

De plus, la conclusion des États généraux de la diplomatie en mars 2023 a donné lieu à l'annonce de 700 ETP supplémentaires au sein du ministère de l'Europe et des affaires étrangères d'ici à 2027. **Une partie de ces effectifs devra accompagner cette montée en puissance de la communication stratégique de notre diplomatie**, principale promotrice de notre stratégie d'influence affirmative.

Recommandation n° 12 : Renforcer les dispositifs de veille et d'alerte au sein du ministère de l'Europe et des affaires étrangères, notamment en :

- développant les capacités de veille et d'enquête en sources ouvertes au sein de la sous-direction « veille et stratégie » de la direction de la presse et de la communication ;
- poursuivant les efforts de formation du réseau diplomatique aux enjeux de communication stratégique.

2. Mobiliser notre audiovisuel extérieur, dans le respect de son indépendance, comme un véritable levier de notre influence positive

a) *Promouvoir le modèle d'une information libre et indépendante, miroir inversé de l'usage des médias comme vecteur d'influence malveillante*

L'audiovisuel extérieur comporte une incontestable dimension d'influence qui doit être renforcé par une amélioration de ses moyens de lutte contre la désinformation, d'une part, et par une plus grande diffusion de ses programmes, d'autre part.

Dans un premier temps, **il importe de renforcer les moyens de notre audiovisuel extérieur pour lutter contre la désinformation**. Le groupe France Médias Monde dispose déjà de capacités de vérification de l'information, avec une quinzaine de programmes dédiés, et diffuse très largement ses contenus sur les réseaux sociaux avec près de 3,7 milliards de vidéos et sons issus des médias de France Médias Monde consommés en 2023. **Deux dispositifs ont été plus spécifiquement développés au sein du groupe**.

D'une part, la rédaction des « Observateurs » de France 24, qui repose sur un réseau de 5 000 correspondants à travers le monde, permet non

seulement une analyse et une démystification des contenus de désinformation, mais est également en mesure d'assurer un travail de veille. Ce réseau se complète d'une cellule de vérification et d'investigation numérique au sein de Radio France Internationale, *InfoVérif*.

D'autre part, France Médias Monde a mis en place **une procédure d'alerte interne de lutte contre les manipulations de l'information visant les institutions démocratiques ou mettant en cause la crédibilité et le professionnalisme de France Médias Monde**. Cette procédure enclenche un travail de vérification et de démystification par les cellules de France 24 et de RFI. En parallèle, France Médias Monde **signale ces alertes auprès des autorités compétentes**, à savoir Viginum et la direction de la communication et de la presse du MEAE. Les résultats des travaux de vérification et d'investigation donnent lieu à une « dissémination » *a posteriori* par des actions de communication, parfois avec le soutien de la direction de la communication et de la presse (DCP).

La mise en place de cette procédure constitue une réaction à des actions de manipulation de l'information visant spécifiquement les médias du groupe France Médias Monde, notamment par des manœuvres d'usurpation de leur identité. Compte tenu de ces évolutions, **la protection d'une information de qualité doit figurer parmi les priorités du prochain contrat d'objectifs et de moyens** de France Médias Monde, actuellement en préparation.

Par ailleurs, la commission note qu'une attention particulière devra être portée aux infrastructures de diffusion des médias de France Médias Monde, notamment en Afrique où elles reposent sur des canaux de diffusion étrangers comme l'a indiqué la présidente-directrice générale, Marie-Christine Saragosse : « *Très présents en Afrique pour la distribution notamment des chaînes TNT, les Chinois nous voient comme un produit d'appel important, et nous affectionnent particulièrement à ce titre* ». Relancée par le rapporteur sur ce point et les risques d'influence malveillante qu'il présente, la présidente-directrice générale a concédé : « *Pour l'heure, nous n'avons pas de problème de censure. Peut-être sommes-nous les faire-valoir d'autres chaînes...* »¹.

Recommandation n° 13 : Renforcer, dans le cadre du prochain contrat d'objectifs et de moyens, les capacités de France Médias Monde pour lutter contre la désinformation.

Dans un second temps, une diffusion plus large de l'audiovisuel extérieur **devrait permettre de diffuser l'influence « affirmative » de la**

¹ [Audition](#) du 6 juin 2024.

France, dans un contexte de concurrence avec des médias affiliés à des États compétiteurs.

La vision d'un audiovisuel extérieur portant un « *contre-narratif* » plus affirmé a été défendue devant la commission d'enquête par Mme Anne-Sophie Avé, Ambassadrice pour le numérique. L'Ambassadrice estime que notre audiovisuel extérieur ne renvoie pas une image positive de la France : « *La BBC a résolument pris le parti de représenter le monde tel que les Britanniques le voient. L'audiovisuel extérieur français présente plutôt la France telle qu'elle se voit elle-même, avec sa diversité, ses contradictions, son goût du débat et même de la polémique. Certains détracteurs de la France entendent ainsi, sur des médias français, des personnes qui tiennent les mêmes propos négatifs, pour ne pas dire dévastateurs, et ils y voient comme la confirmation de leurs propres discours* »¹.

Cette vision plus offensive d'un audiovisuel défendant les positions de la France n'est pas partagée par la présidente-directrice générale de France Média Monde qui estime « *que nous produisons finalement un contre-narratif en racontant, comme nous le faisons au travers d'une multitude de programmes et de situations, des valeurs telles que l'égalité entre les femmes et les hommes, la lutte contre les discriminations, la primauté de la démocratie, la solidarité avec les personnes en situation de faiblesse...* »².

La commission d'enquête partage la position selon laquelle la liberté et l'indépendance de l'audiovisuel extérieur constitue la meilleure arme à opposer des stratégies d'influence agressives. France 24 ou RFI, par leur indépendance leur respect du pluralisme, sont des miroirs inversés de RT, Sputnik ou CGTN. Une des lignes directrices de la lutte contre les influences étrangères malveillantes est de ne rien céder sur notre modèle démocratique. Cette exigence a été réaffirmé par Marie-Christine Saragosse : « *nous devons rester fidèles à notre conception de la démocratie, dont l'information est un des piliers. Heureusement, la démocratie française est un des champions de la liberté d'expression et d'informer ; c'est à cette condition que nous continuerons de recevoir la confiance d'un large auditoire. La France a la réputation d'être championne de la liberté ; il importe qu'elle la conserve et que nous puissions incarner cette indépendance et cette liberté* »³.

Pour ce faire, il est nécessaire de renforcer l'audience de l'audiovisuel extérieur, à destination de l'étranger comme des diasporas présentes sur notre territoire. Comme exposé *supra*, dans la première partie du présent rapport, les diasporas sont des cibles privilégiées pour les opérations d'influence. Or, l'accès à l'information est l'un des principaux leviers du contrôle des diasporas comme de leur instrumentalisation par certains États. Le chercheur de l'Irsem Paul Charon l'a confirmé à propos de la Chine : « *Le média en langue chinoise le plus influent dans notre pays est*

¹ [Audition](#) du 30 avril 2024.

² [Audition](#) du 6 juin 2024.

³ *Idem.*

Nouvelles d'Europe, qui est totalement sous la coupe du PCC. En d'autres termes, les Chinois présents en France et les Français d'origine chinoise qui désirent s'informer en chinois lisent de l'information produite par ce dernier. L'un de nos premiers objectifs devrait être de permettre à la diaspora en France d'avoir accès à une information en chinois qui soit de qualité et qui ne soit pas produite par le PCC »¹. La maîtrise des langues étrangères et la capacité à être entendu de l'autre, compétences spécifiques aux médias à destination de l'étranger, pourraient également s'adresser à des diasporas.

Dans le cas de la Chine, Radio France Internationale dispose de 20 personnes sinophones au sein de sa rédaction, sans compter le réseau de correspondants à l'étranger pouvant maîtriser la langue chinoise. La rédaction alimente deux sites, l'un en chinois traditionnel et l'autre en chinois simplifié, qui recueillent 11 millions de lecteurs et d'auditeurs. Ces capacités pourraient être mobilisées à destination de la diaspora chinoise en France, en complétant ces sites, par une diffusion en radio numérique terrestre (DAB +). Les contenus radiophoniques sinophones de RFI représentant environ deux heures d'antenne par jour, cette diffusion pourrait reposer sur un panachage de programmes en différentes langues. Le coût budgétaire d'une fréquence en DAB + est estimé par FMM entre 10 000 et 20 000 euros par an et par émetteur, soit un montant raisonnable au regard de l'objectif poursuivi.

Recommandation n° 14 : Rendre plus accessible les offres de radio de France Médias Monde en langue étrangère sur le territoire français grâce à la radio numérique terrestre (DAB +).

Outre cette plus nouvelle diffusion sur le territoire français, une extension de l'audience de notre audiovisuel extérieur à l'étranger devrait également être encouragée. Dans un souci de promotion d'un modèle de démocratie ouverte, **il importe de conserver une capacité d'atteindre un plus large public**. Le chercheur David Colon considère qu'en matière d'audiovisuel public « *il nous faut les rendre plus visibles, d'abord en investissant dans ces médias publics. La Chine, aujourd'hui, est en train d'anéantir l'influence de la France et de nombreux autres pays, dans le monde, tout simplement en offrant gratuitement, les services des agences de presse et les productions de China Global Television Network (CGTN). Par conséquent, si nous n'investissons pas, si nous ne réagissons pas à cette menace, nous risquons de voir la voix de la France étouffée, purement et simplement, et ne plus exister, en particulier dans*

¹ [Audition](#) du 6 juin 2024.

les États trop petits privés des moyens nécessaires pour développer leurs propres offres médiatiques »¹.

La diffusion de France 24 en Chine pourrait constituer une opportunité de faire entrer dans ce pays un média pluraliste et indépendant tout en assurant une forme de coopération culturelle sans naïveté aucune.

Recommandation n° 15 : Étendre la diffusion de France 24, notamment en Chine.

Par ailleurs, sur un plan européen, la diffusion de l'audiovisuel public français contribuerait à l'influence positive de notre pays. **L'extension de la production de la chaîne franco-allemande Arte dans d'autres pays européens pourrait être envisagée**, sous la forme d'une « *plateforme européenne de référence* ». Lors de son second discours à la Sorbonne, le 25 avril 2024, le président de la République s'y est déclaré favorable : « *Et je souhaite à ce titre que nous fassions d'Arte, la plateforme audiovisuelle européenne de référence, la plateforme de tous les Européens, qui puisse proposer encore plus qu'aujourd'hui des contenus de qualité distribués dans toutes les langues partout en Europe* »². Cet objectif est poursuivi par la chaîne et son président, Bruno Patino, qui s'est exprimé à plusieurs reprises dans la presse sur cette ambition.

Le projet consisterait, sous la forme d'une plateforme, à **rendre disponible les contenus produits par Arte et ses partenaires dans un plus grand nombre de pays européens**. Ce projet, s'il était décliné dans les pays de l'Est de l'Europe, où l'influence de l'audiovisuel russe est persistante, en raison d'un contournement des sanctions, **renforcer l'influence de la France et du projet européen**.

Recommandation n° 16 : Poursuivre les efforts visant à faire d'Arte une « *plateforme européenne de référence* ».

¹ [Audition](#) du 29 février 2024.

² [Discours du président de la République Emmanuel Macron sur l'Europe à la Sorbonne](#), 25 avril 2024.

b) Une politique d'influence en soutien de l'environnement informationnel de nos partenaires

La lutte contre les opérations d'influence par un soutien aux médias des pays tiers poursuit deux objectifs complémentaires. D'une part, elle permet, **dans une logique d'influence positive, de promouvoir un modèle de presse libre et indépendante**, conforme au respect des valeurs démocratiques de la France. D'autre part, elle permet, en consolidant l'environnement informationnel de ces pays, **de renforcer leur résilience aux influences malveillantes**.

Le ministère de l'Europe et des affaires étrangères mène ainsi une politique de soutien à la liberté de la presse dans les pays en développement. Cette politique est **déclinée dans la « Feuille de route médias et développement » qui fixe notamment un objectif d'appui à la « production d'informations fiables et de qualité »** et d'intensification de la lutte contre la désinformation¹. Elle est principalement mise en œuvre par la direction générale de la mondialisation, de la culture, de l'enseignement supérieur et du développement international et de l'opération Canal France International, avec le soutien du groupe FMM.

La commission d'enquête estime que ces efforts doivent être poursuivis pour renforcer la résilience de l'environnement informationnel de pays partenaires et ainsi **immuniser les médias locaux contre des tentatives de pénétration d'influence**.

3. Pour construire un récit plus affirmé, notre politique d'influence à l'étranger doit davantage s'appuyer sur les ressources de la société civile

Si une politique d'influence ne se décrète pas, elle peut encore moins reposer uniquement sur l'action de l'État. **Le musée du Louvre a sans aucun doute plus contribué que chacune de nos ambassades à l'influence française.** De même que la lutte contre les influences malveillantes ne peut être une réussite qu'en assurant la résilience de la société civile, **la projection d'une influence positive et affirmative ne pourra se faire qu'avec le concours de la société.** Il ne s'agit pas pour la commission d'enquête de recommander une stratégie de « Front uni » à la française mais de souligner que d'autres ressources que notre diplomatie peuvent être mobilisées.

De manière générale, **l'action publique gagne à s'appuyer, sans instrumentalisation aucune, sur la créativité et sur les arts.** À titre d'exemple, à l'occasion de la présidence française du Conseil de l'Union européenne au premier semestre 2022, le journaliste et écrivain Olivier Guez a été à **l'initiative d'un recueil de textes sur les lieux évocateurs de la culture et de**

¹ MEAE, « *Feuille de route Médias et développement 2023-2027* », octobre 2023.

l'histoire européennes¹. Le projet regroupait vingt-sept écrivains contemporains, un par État membre, contribuant ensemble à dresser un autoportrait de l'Europe.

Dans le domaine militaire, l'agence de l'innovation de défense, l'état-major des armées et la direction générale de l'armement ont créé en 2019 une « *red team* » autour d'auteurs, designers, dessinateurs et scénaristes de science-fiction. L'objectif de cette équipe est de nourrir les réflexions opérationnelles et stratégiques des armées dans l'anticipation des guerres de demain.

Dans le même esprit de mobilisation des arts créatifs, **il pourrait être envisagé de créer une « Pléiade d'influence », regroupant des écrivains et des représentants des différentes disciplines artistiques**. La Pléiade originelle regroupait au XVI^e siècle une variété de poètes autour de Pierre de Ronsard, de Joachim du Bellay ou d'Etienne Jodelle notamment, soucieux d'émanciper et d'enrichir la langue française². La « Pléiade d'influence » viserait quant à elle à soutenir l'image de la France à l'étranger, sans tomber dans la propagande, par la promotion de l'esprit de liberté qui caractérise notre pays. Une approche créative permettrait de toucher les cœurs et les esprits en portant un discours positif, en opposition avec les récits portés par les régimes autoritaires, fondés avant tout sur le dénigrement de notre modèle démocratique. Sa production dépasserait le champ discours pour également porter sur les images, au cœur de la perception des individus, comme l'a souligné Mme Cécile Calé, lors de son audition par le rapporteur³.

Loin de constituer une équipe de propagandistes, ce projet reviendrait simplement à réunir ensemble des représentants des arts pour leur faire dire, peindre et exprimer pourquoi ils aiment la France, ce qu'elle doit porter dans le monde et ce pourquoi elle doit être défendue, dans un « autoportrait » à destination du monde.

Recommandation n° 17 : Créer une « Pléiade d'influence » d'écrivains, scénaristes et représentants des différentes disciplines artistiques au service de la politique d'influence et de la diplomatie publique.

¹ Olivier Guez (dir.), *Le Grand Tour. Autoportrait de l'Europe par ses écrivains*, Grasset, 2022.

² Joachim du Bellay, *La défense et illustration de la langue française*, 1549, Gallica, BNF.

³ Audition du rapporteur, 24 juin 2024.

D. RENFORCER LES CAPACITÉS COMMUNES DE DÉTECTION ET DE RIPOSTE DE LA FRANCE ET DE SES ALLIÉS

1. Porter le sujet des influences auprès de nos alliés

Compte tenu de l'avance prise sur la question de la lutte contre les opérations d'influence, la France **devrait poursuivre ses efforts, auprès de ses alliés et dans les forums internationaux**, pour porter cette thématique. Dans le cadre de la prise de conscience de la thématique des influences malveillantes au sein des instances internationales, **la France doit porter cette problématique tout en défendant une plus grande harmonisation normative et une meilleure coordination opérationnelle**.

Sur un plan normatif, il importe de soutenir une plus grande harmonisation des définitions et des concepts, nécessaires à l'élaboration d'une vision commune sur la question des influences étrangères. En particulier, l'absence de définition commune pour les opérations étrangères de manipulation de l'information en ligne est préjudiciable à une compréhension partagée de ce qui constitue aujourd'hui la partie la plus visible des influences malveillantes.

À ce titre, la France **pourrait promouvoir la notion**, établie par le SEAE, de « *Foreign information manipulation and interference* » (FIMI). Cette dernière présente l'avantage d'être très proche de la notion, présente en droit interne, d'ingérence numérique étrangère (INE), à l'exception du critère d'un contenu manifestement inexact ou trompeur, que la commission d'enquête propose de supprimer (recommandation n° 7).

Deux instances pourraient être susceptibles d'adopter la notion de FIMI. D'une part, l'Otan pourrait l'intégrer dans sa doctrine de lutte contre les menaces hybrides. D'autre part, l'OCDE pourrait également s'approprier ce concept. À cet égard, la France co-préside, avec les États-Unis, **le centre de ressources sur la mésinformation et la désinformation de l'OCDE**¹, à l'origine de la publication du récent rapport *Les faits sans le faux* sur la désinformation². La co-présidence de ce centre permet à la diplomatie française de peser dans les recommandations formulées par l'OCDE sur la thématique des influences. L'Ambassadeur Henri Verdier a pu souligner ce point devant la commission d'enquête : « *Nous avions accepté d'en prendre la coprésidence avec les États-Unis, ce qui a entraîné une négociation serrée sur le fait que la régulation des entreprises ferait partie de la réponse et que nous ne pouvions pas nous contenter de transparence et d'autorégulation. Obtenir cette coprésidence sur le fondement de cette vision partagée, âprement négociée, a constitué une véritable victoire diplomatique* »³.

¹ OECD DIS/MIS Resource Hub.

² OCDE, [Les faits sans le faux : Lutter contre la désinformation, renforcer l'intégrité de l'information](#), 2024.

³ [Audition](#) du 28 mars 2024.

À cet égard, l'action des ambassadeurs thématiques, en particulier l'Ambassadrice pour la diplomatie publique en Afrique et l'Ambassadeur pour le numérique, est nécessaire pour porter le sujet des FIMI auprès de nos alliés et des instances internationales. En ce sens, ces ambassadeurs thématiques devraient remettre chaque année un rapport détaillant leur activité conformément aux conclusions de la mission de contrôle de la commission des finances sur ce sujet¹.

Sur un plan opérationnel, il est indispensable de **maintenir une forte implication dans les mécanismes communs de détection et de riposte**.

Au niveau de l'Union européenne, la France participe activement au groupe de travail « résilience contre les menaces hybrides » (ERCHT), qui vise à déterminer une vision partagée des menaces hybrides au sein de l'Union et à recueillir les analyses des différents États membres, y compris des informations classifiées. Ce format permet également l'organisation d'exercices communs entre États membres sur les menaces hybrides. L'organisation d'exercices spécifiquement dédiés à des opérations d'influence malveillante, comme une campagne informationnelle transeuropéenne, devrait être encouragée. De plus, l'investissement de la France auprès du système d'alerte rapide (SAR) du SEAE doit être poursuivi. Il apparaît nécessaire d'inciter l'ensemble des États membres à faire de même. La mobilisation par l'Allemagne, la France et la Pologne, de cet outil dans le cadre du triangle de Weimar à l'occasion des tentatives de manipulation visant des agriculteurs au printemps 2024 est susceptible d'avoir un effet d'entraînement sur les autres États.

Au sein de l'Otan, comme indiqué *supra* dans le II de la deuxième partie, hormis les centres d'excellence sur lesquels s'appuient l'organisation, il n'existe pas de véritable format de coordination opérationnelle pour les États membres. À défaut d'un dispositif d'alerte sur les opérations d'influence, un mécanisme de recensement a posteriori de ces manœuvres permettrait d'identifier leurs caractéristiques spécifiques et de mettre en commun l'expérience des États membres en matière de riposte.

Au sein du G7, le Mécanisme de réponse rapide², créé en 2018 et dont la gestion est assurée par le Canada, constitue un utile forum pour partager, hors de l'espace européen, notamment avec le Japon et les pays anglo-saxons. Pour autant, alors même que ce mécanisme poursuit l'objectif de contribuer à une coordination des membres du G7 dans la réponse aux attaques, il n'y a eu, à la connaissance de la commission d'enquête, aucune mobilisation de cet outil en ce sens. Des manœuvres informationnelles en ligne ont pourtant visé de manière transversale une grande partie des membres du G7, à l'instar de l'opération prochinoise *Spamouflage*.

¹ Rapport d'information n° 726 (2019-2020) fait par Vincent Delahaye et Rémi Féraud, au nom de la commission des finances du Sénat, déposé le 30 septembre 2020.

² Rapid Response Mechanism ou RRM.

Recommandation n° 18 : Amplifier l'engagement de la France pour porter l'enjeu de la lutte contre les « FIMI » au niveau de l'Union européenne, de l'Otan, de l'OCDE et du G7, et renforcer les capacités de riposte collectives.

2. Soutenir la montée en puissance des capacités de détection et de riposte de nos alliés

Comme indiqué dans la partie II du présent rapport, la France a pris, par rapport à ses alliés, **une avance certaine dans le domaine de la lutte contre les influences malveillantes**. Pour ce faire, elle s'est dotée d'instruments et de structures qui pourraient être valorisées auprès de nos partenaires. À cet égard, le modèle de Viginum, service de détection et de caractérisation des manipulations de l'information, pourrait être reproduit à l'étranger.

Il n'existe en effet aucun service strictement équivalent chez nos partenaires. Viginum a pu identifier deux types de structures :

- d'une part, **les structures préexistantes dotées de nouvelles prérogatives pour répondre aux menaces informationnelles**. Il s'agit généralement de structures rattachées aux ministères des affaires étrangères, chargée de la communication stratégique, dont le mandat a été étendu à la détection et à la caractérisation des manipulations de l'information. Cette dernière peut également être confiée à des services de renseignement ;

- d'autre part, **les structures nouvellement créées, sur le modèle de Viginum**.

Le décret n° 2021-922 du 13 juillet 2021 a d'ores et déjà confié à Viginum une mission de liaison opérationnelle et technique avec ses homologues étrangers. **Cette fonction pourrait être déclinée de manière à renforcer les capacités de nos alliés**, tout en intensifiant les partenariats avec les États les plus en pointe.

En ce sens, **l'expérience acquise par le service et ses équipes pourrait être diffusée auprès des États alliés par des actions de formation**. Le triangle de Weimar constitue, par exemple, un format idéal de coopération en faveur d'une **montée en puissance de nos partenaires allemands et polonais**. Une action commune opérationnelle permettrait de dépasser le cadre de simples consultations tripartites. Une telle diffusion de notre modèle présenterait plusieurs avantages :

- un renforcement du niveau global de résilience, par l'émergence d'un réseau de partenaires aptes à mener des actions de détection et à alerter les autres services ;

- la formulation d'un langage commun, par un rapprochement doctrinal et juridique, qui conduirait à une meilleure interopérabilité entre les acteurs de ce réseau. Comme indiqué supra, il n'existe en effet aucune définition unifiée et commune des opérations d'influence malveillantes dans le domaine numérique en Europe.

- mutualisation des connaissances sur l'état de la menace et des nouvelles méthodes utilisées par nos compétiteurs.

Pour ce faire, il appartient à Viginum et au SGDSN de développer des capacités de formation et une « *offre à l'export* » de la « *marque Viginum* ». La France devrait être en mesure de disposer d'un modèle « *clés en mains* » dotée d'une boîte à outils aisée à transposer pour nos partenaires.

De plus, ce travail d'export devra se doubler d'une intensification des collaborations avec les États les plus en pointe sur les questions de manipulation de l'information. Le choix de partenariats pourrait être fondé sur des thématiques géographiques, pour augmenter notre connaissance de certains acteurs hostiles, ou technologiques. Cette collaboration interservices pourrait notamment impliquer des échanges d'agents, sur le modèle pratiqué par le centre de crise et de soutien (CDCS) du ministère de l'Europe et des affaires étrangères, qui accueille chaque année un diplomate allemand.

Recommandation n°19 : Accompagner les partenaires européens souhaitant se doter de capacités comparables à Viginum.

Cette orientation doit également se décliner dans le champ des armées, où le Comcyber a acquis une solide expertise de la lutte informatique d'influence. Par comparaison, la plupart de nos partenaires, s'ils partagent le constat d'une montée en agressivité des stratégies d'influence de nos compétiteurs, ne disposent pas de capacités opérationnelles équivalentes à la France. Des partenariats, fondés sur un accompagnement capacitaire, existent déjà avec certains pays alliés.

Par rapport à l'administration civile et son modèle dual reposant sur un acteur cyber (l'Anssi) et un acteur informationnel (Viginum), le Comcyber intervient dans les deux domaines. La formalisation d'une doctrine de lutte informatique d'influence et son articulation avec la lutte informatique défensive et la lutte informatique offensive offrent un cadre d'intervention clair qui pourrait avantageusement être exporté chez nos partenaires membres de l'Otan.

Recommandation n° 20 : Accompagner les partenaires de l’Otan souhaitant se doter de capacités comparables à celles du Comcyber.

III. DEUXIÈME CERCLE : LA DIFFUSION D’UNE CULTURE DE LA PROTECTION DANS L’ENSEMBLE DE L’ACTION PUBLIQUE

A. LIMITER L’AMPLIFICATION DES OPÉRATIONS D’INFLUENCE DANS LES MÉDIAS ET SUR LES PLATEFORMES

Les médias et des plateformes numériques constituent le vecteur principal des opérations d’influence étrangères malveillantes. Pour cette raison, la stratégie préconisée par la commission d’enquête ne peut faire l’économie d’une réflexion sur les moyens de cette politique.

1. Renforcer les capacités de contrôle par l’Arcom des médias audiovisuels étrangers

Comme cela a été montré *supra* (voir *Deuxième partie, III, A*), les moyens juridiques de l’Arcom pour contrôler les médias étrangers ont été renforcés, tant par la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l’information que par la loi du 21 mai 2024 visant à sécuriser l’espace numérique.

Néanmoins, les travaux de la commission d’enquête ont identifié plusieurs pistes pour renforcer les capacités de contrôle de l’Arcom en la matière.

En premier lieu, le mandat de l’Arcom pourrait être complété, en intégrant directement, à l’article 1^{er} de la loi du 30 septembre 1986 la mention de la prévention des ingérences étrangères parmi les éléments susceptibles de justifier une limitation de la liberté de communication. En pratique, cela permettrait à l’Arcom d’utiliser ses pouvoirs (mise en demeure, sanction *etc.*) à l’encontre d’un média, extra-européen ou non, qui se ferait le relai d’une opération d’ingérence étrangère dans le débat public. En l’état du droit, cette thématique ne peut être appréhendée qu’indirectement au travers de celles, déjà prévues par la loi, de la sauvegarde de l’ordre public ou encore de l’honnêteté et de l’indépendance de l’information. Il est d’ailleurs à noter que le dispositif institué par la loi du 22 décembre 2018 permettant à l’Arcom de suspendre la diffusion d’une chaîne étrangère se livrant à des opérations de désinformation en contexte électoral a déjà, *de facto*, élargi le mandat de l’Arcom à cette thématique dans le cadre de cette procédure particulière. Pour exercer cette compétence, l’Arcom pourrait

s'appuyer sur la convention cadre de partenariat signée le 4 juillet 2024 entre l'Arcom et Viginum. En tout état de cause, l'utilisation des pouvoirs de régulation resterait décidée par l'autorité indépendante, sous le contrôle du juge administratif.

En deuxième lieu, le rétablissement d'une obligation de conventionnement pour l'ensemble des médias extra-européens relevant de la compétence de l'Arcom serait souhaitable, l'existence d'une telle convention constituant une garantie pour le public. Pour mémoire, cette obligation avait été supprimée par une loi de 2006¹ dont l'objectif, paradoxalement, était de permettre de suspendre plus rapidement la diffusion chaînes étrangères dont les contenus faisaient l'apologie du terrorisme. Entre temps, le droit a évolué et la loi du 22 décembre 2018 a notamment permis à l'Arcom de demander au président de la section du contentieux du Conseil d'État qu'il ordonne en référé à l'opérateur satellitaire de faire cesser la diffusion d'un contenu ou la distribution d'un média extra-européen si ce service porte atteinte aux intérêts fondamentaux de la Nation, dont le fonctionnement régulier de ses institutions, notamment par la diffusion de fausses informations. Une telle évolution, qui suppose une **modification de l'article 33-1 de la loi du 30 septembre 1986**, concourrait à atteindre l'objectif proposé par Reporters sans frontières, lors de son audition par la commission d'enquête², d'assurer une égalité de traitement entre tous les médias audiovisuels au sein de l'Union européenne.

Enfin, une simplification des critères de détermination de la compétence du régulateur serait souhaitable. En l'état, comme cela a été rappelé, l'**article 2 de la directive SMA** fixe comme critère principal celui de la localisation de la liaison montante entre le lieu d'émission du service et le satellite chargé d'en assurer la diffusion, et comme critère secondaire celui de la nationalité de la capacité satellitaire. Ses règles sont sources de complexité, comme le Président de l'Arcom l'a exposé lors de son audition devant la commission d'enquête. Dans ses réponses au questionnaire du rapporteur, l'Arcom précise en effet que ces règles soulèvent une difficulté liée à la volatilité de la localisation de liaison montante vers le ou les satellites de diffusion et suggère que l'ordre des critères soit inversé afin de privilégier la nationalité de la capacité satellitaire. **Une telle simplification pourrait être prévue dans le cadre d'une prochaine révision de la directive SMA.**

¹ Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

² [Audition](#) du 10 juin 2024.

Recommandation n° 21 : Compléter le mandat de l'Arcom pour y intégrer la thématique de la prévention des ingérences étrangères.

Recommandation n° 22 : Rétablir une obligation de conventionnement avec l'Arcom pour les médias audiovisuels extra-européens.

Recommandation n° 23 : À l'occasion d'une prochaine révision de la directive « SMA », proposer une simplification de l'application des critères utilisés pour déterminer l'État membre compétent au titre d'un média audiovisuel extra-européen.

2. Assumer une politique ambitieuse de régulation de l'espace numérique

La nocivité des grandes plateformes, qui constituent par nature, du fait de leur modèle économique, un terreau fertile pour le déploiement d'opérations d'ingérences étrangères.

La stratégie de lutte contre les influences étrangères se doit de penser ce problème majeur dans toutes ses composantes, en se dotant d'une vision claire des objectifs de moyen et de court-terme, et en définissant un ordre d'actions précis.

a) Dans l'immédiat, prendre des mesures pour renforcer la protection du débat public numérique français

En l'état du droit, un seul dispositif législatif contraignant permet de protéger le débat public numérique français en cas d'opération d'ingérence numérique étrangère en dehors du cas spécifique de médias sous sanction européenne.

Pour mémoire, il s'agit du **dispositif prévu à l'article L. 163-2 du code électoral** permettant à l'autorité judiciaire saisi par le procureur ou par toute personne mentionnée par cet article ou ayant intérêt à agir, au cours des trois mois qui précèdent un scrutin, de demander à ce que les plateformes fassent cesser la diffusion de contenus de désinformations diffusées de façon massive et artificielle.

Ce dispositif comporte deux caractéristiques essentielles :

- il est limité à la période des trois mois précédant un scrutin ;

- il est limité à la diffusion d'informations qui satisfont les deux critères cumulatifs suivants : leur caractère faux ou trompeur de nature à altérer la sincérité d'un scrutin des informations (*i*) et le caractère massif et

artificial de cette diffusion (ii), et ce indépendamment de tout rattachement à la caractérisation d'une ingérence étrangère ;

La commission d'enquête considère que, s'agissant d'ingérences numériques étrangères, le cantonnement du dispositif à la seule période électorale n'est pas pleinement satisfaisant, en ce qu'elle est mal adaptée à la menace. Le cas des ingérences étrangères constatées dans le cadre de la crise en Nouvelle-Calédonie montre bien que celles-ci peuvent porter une grave atteinte aux intérêts fondamentaux de la Nation en dehors des contextes électoraux.

Pour cette raison, il préconise l'adoption d'un second dispositif d'inspiration similaire de cessation de diffusion d'informations sur décision du juge qui :

- ne serait pas limité, dans son application, à la période électorale mais devrait concerner des contenus rattachables à des opérations d'ingérence numérique étrangères caractérisées ;

- conserverait les mêmes deux critères cumulatifs concernant la caractérisation des informations diffusées, à ceci près que leur caractère faux ou trompeur devrait être de nature non pas à altérer la sincérité du scrutin, mais à porter atteinte aux intérêts fondamentaux de la Nation.

En période électorale, le dispositif de l'article L. 162-3 du code électoral, de portée plus large puisque non limité aux opérations d'ingérence numérique étrangères, continuerait de s'appliquer.

Recommandation n°24 : Sur le modèle du dispositif prévu à l'article L. 163-2 du code électoral, mettre en place un dispositif permettant à l'autorité judiciaire de faire cesser la diffusion massive et artificielle de contenus faux ou trompeurs rattachables à une ingérence numérique étrangère et de nature à porter atteinte aux intérêts fondamentaux de la Nation.

b) À court terme mettre pleinement en œuvre le DSA pour lutter contre les influences étrangères malveillantes sur les plateformes

Si l'approche retenue par le DSA ne saurait être pleinement satisfaisante, celui-ci recèle néanmoins des potentialités intéressantes pour renforcer la lutte contre les opérations d'ingérence numérique étrangères.

La commission d'enquête a entendu les représentants des affaires publiques pour la France de quatre grandes plateformes : Meta¹,

¹ [Audition](#) du 23 mai 2024.

Google/Youtube¹, X (ex-Twitter)² et TikTok³. Ces auditions ont témoigné que les plateformes ont pleinement intégré, dans leur communication publique, la nécessité de mettre en avant l'existence d'actions destinées à lutter contre la désinformation. **Cette évolution des discours témoigne bien du fait qu'avec de la volonté politique, le législateur européen est bien en mesure de peser dans le rapport de forces engagé avec les plateformes.**

Certes, dans les faits, la réalité est plus nuancée. Si la procédure n'est pas encore menée à son terme, l'avis préliminaire de non-conformité au DSA adressé par la Commission européenne par X (ex-Twitter) illustre bien l'existence de problématiques importantes et persistantes (voir *supra*).

Comme cela a également été rappelé, la coopération des plateformes avec Viginum est encore inégale et, à ce jour, seul Google/Youtube a offert un accès API à ses agents.

Se pose notamment à cet égard la question des moyens concrets que se donnent les plateformes pour se conformer au DSA.

Dans ses réponses au questionnaire du rapporteur, la plateforme X (ex-Twitter) a indiqué qu'en avril 2024, la direction *Safety* supervisait une équipe d'environ 1 700 personnes travaillant dans la modération de contenu, parmi lesquels 52 personnes dont la langue principale est le français.

Interrogées par écrit sur leurs moyens en la matière, les plateformes ont indiqué au rapporteur :

- s'agissant de X (ex-Twitter), en avril 2024, la direction *Safety* supervisait une équipe d'environ 1 700 personnes travaillant dans la modération de contenu, parmi lesquels 52 personnes dont la langue principale est le français

- s'agissant de Meta, les équipes compétentes comptent également 40 000 personnes, dont 15 000 au titre de Facebook. Dans ses réponses, Meta a ajouté avoir constitué, pour contrer les opérations d'influence clandestines, « *des équipes mondiales spécialisées pour identifier les comportements inauthentiques coordonné* » ;

- s'agissant de TikTok, les équipes *Trust and Safety* comptent 40 000 personnes, parmi lesquels 650 modérateurs francophones ;

- Google/Youtube n'a pas répondu au questionnaire du rapporteur. Lors de son audition, le directeur des relations institutionnelles de Youtube a néanmoins indiqué que 20 000 personnes travaillaient sur les enjeux de modération⁴.

¹ [Audition](#) du 28 mai 2024.

² [Audition](#) du 30 mai 2024.

³ [Audition](#) du 4 juin 2024.

⁴ [Audition](#) du 28 mai 2024

En ce qui concerne les modérateurs, Tariq Krim, fondateur du laboratoire d'idées Cybernetica a indiqué, lors de son audition par la commission d'enquête qu'il fallait néanmoins garder à l'esprit que : « *en général les personnes qui s'occupent de ces tâches ne font pas partie des plateformes. [Celles-ci] utilisent des entreprises implantées aux Philippines ou dans le centre des États-Unis. Les opérateurs voient tous les immondices de la planète, ce que personne ne doit voir, et ont souvent des chocs psychologiques (...) Les plateformes cherchent à utiliser l'intelligence artificielle pour limiter ce travail, cela fonctionne mais pas complètement* »¹.

S'agissant des actions concrètes des plateformes, la commission d'enquête ne peut que regretter que l'Arcom n'ait pas encore publié de rapport bilan sur les actions des plateformes en matière de lutte contre les manipulations de l'information depuis celui relatif à l'année 2021, qui date de la fin de l'année 2022, alors même que celui-ci constitue une source d'information et de recommandations précieuses.

La commission considère qu'il est donc indispensable de mobiliser pleinement en œuvre les outils conférés par le DSA, aussi bien au niveau national qu'européen. Cela suppose notamment :

- d'accorder une vigilance particulière aux moyens concrets que se donnent les plateformes pour lutter effectivement contre les manipulations de l'information et la publicité ciblée détournée dans le cadre d'opérations d'influence étrangères malveillantes ;

- de veiller à ce que le régulateur national dispose bien des moyens de mettre pleinement en œuvre ses compétences de contrôle des plateformes, ce qui passe par un renforcement de ses moyens, et puisse en rendre compte au travers de la remise annuelle du rapport relatif au bilan des mesures prises par les plateformes : en l'état du droit, il est simplement prévu que la remise de ce rapport soit seulement « *périodique* »² ;

- d'encourager les plateformes à mettre en place des mesures permettant effectivement de promouvoir la qualité de l'information diffusée. En termes méthodologiques, elles devraient être plus fortement incitées à s'appuyer sur le *Journalism Trust Initiative* (voir *Deuxième partie, III, A*).

En matière de lutte contre les hypertrucages (*deep fakes*), les plateformes pourraient en outre être encouragées à développer des technologies dites de « *tatouage numérique* » (*digital watermarking*), qui permettent d'attester de l'authenticité d'un contenu numérique. Pourrait également être explorée dans ce cadre la piste proposée lors de son audition par David Chavalarias, évoquée précédemment, et consistant à permettre aux utilisateurs de s'authentifier en tant que Français, tout en restant anonyme, sans donner d'autres d'informations - par exemple en passant par un intermédiaire comme France Connect, de telle sorte que les utilisateurs

¹ [Audition](#) du 4 juin 2024.

² Article 58 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

pourraient ainsi filtrer les contenus en disant qu'ils ne veulent voir que les contenus émis par leurs compatriotes, ce qui permettrait d'éliminer de nombreuses ingérences propagées à partir de faux comptes.

Il appartiendra également au régulateur de s'assurer que les plateformes, dans le cadre des obligations qui leur sont imposées par le DSA, se donnent effectivement les moyens de détecter et supprimer les contenus consistant à usurper l'identité visuelle d'un média existant.

Interrogée par le rapporteur sur la question de ses moyens, l'Arcom, dans ses réponses au questionnaire, a indiqué que : « *l'Arcom a beaucoup renforcé ses équipes en charge de la régulation des plateformes en ligne, en particulier grâce aux moyens humains et financiers complémentaires qui lui ont été accordés par le Parlement au titre des lois de finances pour 2023 et 2024. Elle s'est ainsi dotée en février 2021 d'une direction des plateformes en ligne dont les effectifs, en croissance, s'élèvent aujourd'hui à une douzaine d'agent. (...) Les exigences liées à la bonne mise en œuvre de cette régulation justifient de poursuivre, dans les années à venir, la montée en puissance des moyens qui y sont affectés, sans qu'il soit possible à ce stade de quantifier précisément les besoins. La mise à contribution légitime de l'Arcom à l'amélioration de la situation des finances publiques est toutefois susceptible d'entraver ce mouvement, malgré les efforts de redéploiement interne que l'Autorité a engagés*

 ».

c) *À moyen terme : porter, au niveau européen, une ambition de réforme du statut des plateformes*

Comme cela a été rappelé *supra*, l'approche retenue par le DSA, fondée sur une simple obligation de moyens pour les plateformes, reste trop timorée et n'est pas à la hauteur des enjeux (voir *Deuxième partie, II, A*).

À moyen-terme, un consensus se dégage parmi les membres de la commission d'enquête pour porter, au niveau européen, une position tendant résolument à réformer le statut des plateformes, qui, cela a été largement montré, ne sauraient être considérées comme de simples « hébergeurs » des contenus.

Il s'agit d'une **préoccupation ancienne du Sénat** qui a déjà formulé cette recommandation à de multiples reprises. Celle-ci a notamment été portée dès 2021 par une résolution européenne adoptée par le Sénat sur une initiative de Florence Blatrix-Contat et Catherine Morin-Desailly, qui « *[déplorait] que le règlement [sur les services numériques] ne remette pas en cause le principe de responsabilité limitée des hébergeurs, y compris des plateformes et des très grandes plateformes en ligne* » ; et « *[appelait] à nouveau à créer un régime européen de responsabilité renforcée* » pour celles-ci¹.

¹ [Rapport d'information n° 274 \(2021-2022\)](#) fait par Florence Blatrix-Contat et Catherine Morin-Desailly au nom de la commission des affaires européennes du Sénat sur la proposition de législation européenne sur les services numériques, déposé le 8 décembre 2021 ; [Résolution n° 70 \(2021-2022\)](#), devenue résolution du Sénat le 14 janvier 2022.

Le Sénat avait également voté, la même année dans le cadre de l'examen du projet de loi confortant le respect des principes de la République, un amendement du Président Claude Malhuret tendant à conférer à celle-ci le statut d'éditeur, au même titre que les médias régis par la loi du 29 juillet 1881 relative à la liberté de la presse, au titre des contenus qu'elles proposent à leurs utilisateurs par le biais non de ses abonnements propres mais d'un traitement algorithmique.

Au terme de cet amendement, finalement non retenu dans le texte finalement adopté, les plateformes seraient ainsi « *civilement et pénalement responsables des informations qu'elles stockent pour mise à disposition du public, dès lors qu'elles effectuent sur ces informations un traitement par algorithme, modélisation ou tout autre procédé informatique, afin de classer, ordonner, promouvoir, recommander, amplifier, ou modifier de manière similaire la diffusion ou l'affichage de ces informations, à moins qu'il ne soit chronologique, alphabétique, aléatoire, ou fondé sur la quantité ou la qualité des évaluations attribuées par les utilisateurs* »¹.

Cette position a été réaffirmée s'agissant de la plateforme TikTok dans le cadre de la commission d'enquête du Sénat consacrée à cette plateforme².

Deux pistes peuvent être mises sur la table à cet égard, et portées par la France au niveau européen.

La première serait de conférer aux plateforme le statut d'éditeurs, et de les rendre pleinement responsables des contenus diffusés au moyen d'une méthode de ciblage reposant sur un procédé informatique, en s'inspirant des critères de l'amendement mentionné *supra*. Il convient cependant de relever que cette piste, qui était au cœur des débats lors de l'examen du DSA, n'a pas permis de rassembler une majorité au Parlement européen et parmi les États membres.

Une seconde option, préconisée par les représentants de Reporters sans frontières leur de leur audition, consisterait à instituer un statut hybride et *ad hoc*, qui resterait à construire, d'« *entités structurantes de l'espace informationnel* ». Selon ces derniers : « *même si elles s'approchent par certaines dimensions du statut d'éditeur et par d'autres de celui d'hébergeur, il ne faut ni déresponsabiliser les plateformes ni en faire les rédacteurs en chef du monde. C'est toute la complexité de la chose* »³.

Il s'agirait d'une forme de « ni-ni » : ni simple hébergeur, ni éditeur.

N'étant pas éditeurs, elles ne seraient par principe pas responsables des contenus diffusés.

¹ [Amendement n° 250 rect sexies](#) déposé sur le texte de la commission n° 455 (2020-2021) au stade de la première lecture au Sénat, intégré à l'article 19 bis AA du texte n° 94 (2020-2021) adopté.

² [Rapport d'information n° 831 \(2022-2023\)](#) fait par Claude Malhuret au nom de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence, déposé le 4 juillet 2023.

³ [Audition](#) du 13 juin 2024.

N'étant pas simples hébergeurs, elles pourraient se voir appliquer des obligations spécifiques qui ne se limiteraient pas à des obligations de moyens comme c'est le cas dans le cadre de la logique du DSA. À titre d'exemple, la promotion de contenus sur la base de la *Journalism Trust Initiative*, ou d'une autre norme à définir, pourrait désormais leur être imposée. De même, ce cadre pourrait permettre de donner obligation aux plateformes de vérifier le nom des sites, pages et comptes lors de l'inscription, et refuser tout nom de site ou de page qui emprunteraient le nom et le logo d'un média existant.

En tout état de cause, il convient de souligner que les contenus liés aux ingérences étrangères ne se limitent pas à de la désinformation - les opérations de manipulation et de diffusion massive peuvent dans certains cas porter sur des informations qui ne sont pas fausses - et que la désinformation n'est pas en soi illicite. Ainsi, la question du statut des plateformes, et en particulier celle de leur responsabilité civile et pénale vis-à-vis des contenus, ne saurait résoudre l'ensemble de la question. In fine, l'approche consistant à développer la résilience de la population (voir *infra*), doit primer sur l'approche régulatoire.

d) Pour s'attaquer à la racine du problème, la nécessité d'agir résolument en faveur de la souveraineté numérique française et européenne

Au plan structurel, il convient de rappeler que la racine du problème réside dans le fait que notre espace informationnel est en pratique structuré par des outils numériques, les grandes plateformes, qui sont pour l'essentiel d'origine extra-européenne et qui reposent fondamentalement sur un modèle économique nocif ainsi que sur des valeurs qui ne sont pas les nôtres.

La régulation reste possible, le DSA le montre, mais ne permet pas de remédier à une forme de vice de construction de ces plateformes.

Aussi, la commission d'enquête tient à souligner que la seule solution positive et structurelle de long terme pour l'Europe est celle qui consiste à trouver le moyen de sortir enfin de l'état de « *colonie du monde numérique* », pour reprendre l'expression d'un rapport fait par Catherine Morin-Desailly au nom de la commission des affaires européennes du Sénat il y a désormais plus de dix ans, mais dont le constat reste en large partie vérifié¹.

Comme le résume bien Bernard Benhamou lors de son audition par la commission d'enquête : « *nous ne pouvons pas être uniquement sur un rôle défensif, avec tout le respect que j'ai pour les textes importants qui ont été adoptés : règlement sur les services numériques (DSA), règlement sur les marchés numériques (DMA), règlement sur la gouvernance des données (DGA) ou règlement sur*

¹ [Rapport d'information n° 443 \(2012-2013\)](#) fait par Catherine Morin-Desailly au nom de la commission des affaires européennes du Sénat, sur « *l'Union européenne, colonie du monde numérique ?* », déposé le 20 mars 2013.

l'intelligence (AIA)... Nous devons être en mesure de développer une politique volontariste à l'échelle de l'Union européenne sur les segments critiques, dont l'intelligence artificielle qui deviendra d'un point de vue industriel un élément central des stratégies des différents blocs. Si nous ne le faisons pas, toutes les mesures de régulation seront contournées. La politique industrielle est un élément clé de la régulation de ce secteur »¹.

L'atteinte de cet objectif de long terme passe nécessairement par une stratégie de politique industrielle adaptée, dont la détermination des éléments précis excède toutefois le champ de la commission d'enquête. Lors de son audition Bernard Benhamou prône notamment la mobilisation de la commande publique, qui pourrait être favorisée au moyen d'un *European Business Act*, sur le modèle du *Small Business Act* états-unien qui permettrait de réserver certains marchés publics aux petites entreprises nationales. Mobiliser ainsi le levier de la commande publique permettrait de donner priorité aux acteurs français et européens avant de conclure avec un opérateur étranger. En particulier, l'hébergement des données de santé, l'équipement des ministères sensibles doivent l'objet d'une vigilance particulière.

Une telle politique doit se fixer pour objectif de long terme de se doter de capacités françaises et européennes tant sur les segments *software* que *hardware*, notamment d'informatique en nuage (*cloud*), et ce prioritairement pour l'équipement des entités publiques : État, Parlement, collectivités territoriales, hôpitaux, établissements d'enseignement supérieur et de recherche etc.

¹ [Audition](#) du 4 juin 2024.

Recommandation n° 25 : À court terme, exploiter pleinement les nouvelles prérogatives de régulation conférées par le règlement de l'Union européenne sur les services numériques (DSA) pour s'assurer que les plateformes se donnent les moyens de lutter contre les manipulations de l'information liées à des opérations d'ingérences informationnelles.

Recommandation n° 26 : À moyen terme, porter au niveau européen une position tendant à conférer aux plateformes un statut d'éditeur au titre d'une partie des contenus qu'ils diffusent ou, à minima, leur conférer un statut hybride d'« *entités structurantes de l'espace informationnel* » (ni-hébergeur, ni éditeur) assorti d'obligations spécifiques permettant de prévenir les ingérences informationnelles.

Recommandation n° 27 : Se donner les moyens d'une politique industrielle volontariste en faveur de la souveraineté numérique française et européenne, avec pour objectif de long terme que notre espace informationnel cesse d'être structuré par des opérateurs extra-européens.

Au plan prospectif, plusieurs autres pistes peuvent être esquissées pour assainir l'espace numérique.

En premier lieu, au vu de l'importance stratégique déterminante prise par les données et l'IA, dont les opérations d'ingérences étrangères ne constituent qu'une illustration parmi d'autres, la France et l'Europe se doivent d'agir pour mettre un frein aux stratégies de puissance débridées dans l'espace numérique et faire en sorte qu'en tant qu'arme 2.0, l'IA soit enfin saisie par le droit international public au moyen d'un véritable traité sur international sur l'IA.

L'Europe a ouvert la voie, à cet égard, avec l'adoption récente de deux instruments importants :

- le règlement de l'Union européenne du 13 juin 2024 sur l'intelligence artificielle sur l'intelligence artificielle¹ ;

- la convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit adoptée dans le cadre du Conseil de

¹ Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)

l'Europe le 17 mai 2024 et sera ouvert à la signature des États à compter du 5 septembre 2024¹.

Il est à noter que ce dernier traité, qui comporte une stipulation interdisant les usages de l'IA destinés à saper les processus démocratiques, notamment *via* des opérations de désinformation, sera ouvert à la signature de l'ensemble des États, y compris au-delà du Conseil de l'Europe. Il pourra donc être opportun de s'appuyer sur cet instrument.

Un second enjeu prospectif identifié concerne la mémoire et la préservation de la vérité historique dans l'espace numérique, alors que les potentialités falsificatrices de l'IA peuvent être mises au service de narratifs mensongers déployés par des puissances révisionnistes. la France et l'Europe se doivent d'agir pour éviter la falsification des archives de l'Internet, ce qui suppose une plus grande souveraineté sur ses structures.

Lors de son audition, Tariq Krim a partagé avec la commission d'enquête des réflexions stimulantes en la matière :

« Si vous cherchez en Chine, sur l'internet chinois, des informations sur Jack Ma, qui est l'équivalent de Jeff Bezos, l'un des entrepreneurs les plus connus, il n'y a plus aucune occurrence, il a disparu. Nous sommes dans un monde où, avec la censure [sur Internet], il n'y a pas de mémoire. (...) Or, aujourd'hui, la mémoire du web français, c'est « archive.org » aux États-Unis. Que se passera-t-il si demain Wikimedia disparaît et que nous n'avons plus que les IA génératives pour répondre à telle ou quelle question ? »

L'un des antidotes est de s'assurer de conserver une archive numérique de qualité. (...) La question de la mémoire est fondamentale puisqu'avec les images générées peut-être que dans dix ans, le monde réel, ce que j'appelle parfois l'internet analogique, qui est en lien avec une réalité du monde, sera ultra-minoritaire dans le nouvel Internet. Dans ce nouvel Internet, rechercher la vérité, ce sera finalement comme des fouilles archéologiques aujourd'hui, c'est-à-dire aller chercher dans des milliards de données synthétiques les données qui seront réelles et dont seule une partie correspondra à la vérité.

Il faut donc préserver la mémoire, préserver les archives correspondant aux textes originaux (...) Si dans quelques années nous ne sommes plus capables d'identifier les éléments qui sont factuellement, les ingérences seront d'une implacable efficacité »².

3. Promouvoir un environnement informationnel de qualité

Comme cela a été évoqué, dans une démocratie comme la nôtre, l'assainissement de l'espace médiatique relève en large partie des médias eux-

¹ Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit adoptée dans le cadre du Conseil de l'Europe

² [Audition](#) du 4 juin 2024.

mêmes. Cependant, l'État peut jouer un rôle d'impulsion et de soutien précédemment (voir *Deuxième partie, III, A*).

En particulier, la création d'un Observatoire des influences étrangères malveillantes préconisée par la commission d'enquête (voir *recommandation n° 6*), qui serait largement ouvert aux journalistes, permettrait d'améliorer leur appréhension du phénomène, et de mettre à jour leurs connaissances en la matière, ainsi que de partager des bonnes pratiques avec leurs confrères ainsi qu'avec les acteurs du monde académique.

Un autre levier d'action, identifié par la directrice générale des médias et des industries culturelles (DGMIC) lors de son audition, réside dans le conventionnement avec les médias réalisant des missions d'intérêt général, et en particulier ceux du service public audiovisuel.

Néanmoins, comme la commission d'enquête a pu le relever, ces conventions d'objectifs et de moyens ont tendance à traiter la problématique de la désinformation de façon générale, sans aborder explicitement la question des ingérences étrangères, alors que celles-ci comportent des objectifs spécifiques et induisent des modes opératoires particuliers, parmi lesquelles l'usurpation de l'identité visuelle de ces médias, comme dans le cadre des attaques subies par France Médias Monde ou encore des opérations *RRN/Döppleganger* mises en œuvre par des acteurs pro-russes.

À titre d'exemple, France Médias Monde a mis en place une procédure d'alerte en cas d'attaque contre ses chaînes, notamment par une opération d'usurpation visuelle. Il est fait référence à cette procédure dans le rapport annuel d'exécution au titre de l'année 2023 du contrat d'objectifs et de moyens signé entre l'État et France Médias Monde.

Sans interférer sur la ligne éditoriale de ces médias, la commission d'enquête considère que les contrats d'objectifs et de moyens passés entre l'État et les médias réalisant des missions d'intérêt général pourraient plus spécifiquement traiter la question des ingérences étrangères, notamment en prévoyant la mise en place de dispositifs internes de protection et d'alerte.

Recommandation n° 28 : Identifier spécifiquement les menaces liées aux ingérences étrangères dans les contrats d'objectifs et de moyens passés entre l'État et les médias réalisant des missions d'intérêt général, en prévoyant notamment la mise en place de dispositifs internes de protection sur le modèle de la procédure d'alerte mise en place par France Médias Monde.

B. RENFORCER LES INSTRUMENTS DE CONTRÔLE DE LA VIE PUBLIQUE ET POLITIQUE À L'AUNE DU RISQUE D'INGÉRENCE

1. Combler les lacunes du cadre juridique régissant le financement de la vie politique et donner de nouveaux moyens d'enquête à la CNCCFP

Les travaux de la commission d'enquête ont permis de mettre en évidence **un certain nombre de lacunes dans le cadre juridique régissant le financement de la vie politique** (voir *Deuxième partie, III, B*).

En particulier, il convient de remédier :

- à l'**absence de condition de nationalité ni de résidence en matière de prêt des personnes physiques** à un candidat à des élections ou à un parti politique, qui font courir des risques directs d'ingérence étrangères ;

- à l'**absence de plafond de ces prêts**, ce qui, même si une condition de nationalité leur était appliquée, peut comporter des risques de dépendances vis-à-vis de certains intérêts particuliers, qui peuvent eux-mêmes être en lien avec les intérêts d'une puissance étrangère ;

- à l'**absence de condition de nationalité ni de résidence en matière de cotisation** des personnes physiques aux partis politiques.

Par ailleurs, le droit en vigueur ne permet pas d'appréhender certaines activités des candidats et des partis sur les plateformes numériques, et des pratiques éventuelles de rémunérations des créateurs de contenus (ou « influenceurs »), qui peuvent être de nationalité française ou étrangère. De telles pratiques devraient être interdites, comme le préconise la Commission nationale des comptes de campagne et des financements politiques (CNCCFP).

La CNCCFP a également fait part à la commission d'enquête de la nécessité, pour mener à bien ses missions, de pouvoir s'assurer que le prêteur ne serve pas d'intermédiaire pour dissimuler l'origine réelle des fonds apportés, et qu'elle ne masque pas ainsi un financement prohibé.

Dans ce même souci de renforcer les prérogatives de la CNCCFP, la commission d'enquête souscrit à plusieurs autres propositions formulées par celle-ci, en lui permettant notamment **d'accéder au fichier national des comptes bancaires (Ficoba)**.

La CNCCFP a également exprimé le souhait de pouvoir « saisir » Tracfin pour pouvoir obtenir, le cas échéant, des renseignements utiles à ses investigations. Cette proposition est d'ailleurs reprise par le rapport de la commission d'enquête de l'Assemblée nationale relative aux ingérences étrangères (recommandation n° 10)¹.

La commission d'enquête relève cependant que cette recommandation se heurte à une limite tenant au bon fonctionnement de Tracfin. Interrogé sur ce point lors de son audition devant la commission d'enquête, son directeur a ainsi déclaré : « *je ne souhaiterais pas que quiconque ait la faculté de nous obliger à travailler tout de suite sur tel ou tel dossier. Si n'importe qui peut requérir Tracfin, le législateur doit décider que la définition de nos priorités dépend de nos fournisseurs, et non de nous - donc que les terroristes passent en bas de la liste des priorités*² ».

En revanche, la commission d'enquête considère que **la CNCCFP pourrait utilement être ajoutée à la liste des personnes, limitativement énumérées à l'article L. 561-31 du code monétaire et financier, à qui Tracfin est autorisé à transmettre des informations**.

¹ [Rapport n° 1311 \(seizième législature\)](#) fait par Constance Le Grip au nom de la commission d'enquête de l'Assemblée nationale relative aux ingérences politiques, économiques et financières de puissances étrangères - États, organisations, entreprises, groupes d'intérêts, personnes privées - visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français, déposé le 1^{er} juin 2023, Tome I.

² [Audition](#) du 30 mai 2024.

Recommandation n° 29 : Combler les lacunes existantes dans le cadre juridique applicable au financement des campagnes électorales et des partis politiques, en limitant le montant des prêts à un candidat ou à un parti politique, en interdisant aux personnes physiques étrangères ne résidant pas en France de consentir à ce type de prêts, et en interdisant aux mêmes personnes de cotiser aux partis politiques.

Recommandation n° 30 : Interdire aux partis et aux candidats de recourir aux créateurs de contenus sur les plateformes (« influenceurs ») pour mener des campagnes d'influence électorale rémunérées.

Recommandation n° 31 : Renforcer les prérogatives de la Commission nationale des comptes de campagnes et des financements politiques (CNCCFP), en lui permettant de demander aux prêteurs d'établir l'origine des fonds prêtés à un candidat ou à un parti politique, d'accéder au fichier national des comptes bancaires (Ficoba) et en l'intégrant à la liste des personnes à qui Tracfin peut transmettre des informations.

2. Donner à la HATVP les moyens de pleinement mettre en œuvre ses nouvelles missions en matière de contrôle des influences étrangères et veiller à préserver le haut niveau d'exigence de ce régime

a) Donner à la HATVP les moyens de mettre en œuvre les nouvelles missions qui lui ont été confiées par la loi visant à prévenir les ingérences étrangères en France

La commission d'enquête a salué l'adoption de la loi visant à prévenir les ingérences étrangères en France, dite loi « Ingérences étrangères », qui a permis de conférer à la HATVP de nouvelles prérogatives importantes en matière :

- la création et la gestion d'un répertoire national des représentants d'intérêts agissant pour le compte de mandants étrangers ;

- l'exercice d'un contrôle sur les risques d'influence étrangère en matière de reconversion professionnelle des responsables publics dans le secteur privé ;

- un contrôle des informations relatives aux financements étrangers perçus par les laboratoires d'idées (*think tanks*).

Cependant, comme cela a été rappelé *supra* (voir *Deuxième partie, III, B*), l'exercice de ces nouvelles missions suppose inévitablement des moyens supplémentaires, alors même que ceux de la HATVP sont aujourd'hui taillés au plus juste. En particulier, la création du nouveau répertoire implique inévitablement certains développements informatiques coûteux.

Une telle augmentation de moyens découle expressément de la volonté exprimée par le législateur. Les travaux préparatoires l'attestent, puisque lors de l'examen de la proposition de loi dont ce texte est issu en commission mixte paritaire, le co-rapporteur Sacha Houlié : « *L'Assemblée nationale avait prévu une entrée en vigueur au 1^{er} janvier 2024. Le Sénat avait préféré la date du 1^{er} janvier 2025. Nous avons retenu, avec Agnès Canayer, le 1^{er} juillet 2025 pour plusieurs raisons. Cela permettra de voter des crédits pour la HATVP, de recruter des agents et de s'assurer que ceux-ci soient opérationnels six mois après l'adoption du projet de loi de finances pour 2025* »¹.

La commission d'enquête appelle donc à ce que le prochain projet de loi de finances vienne tirer les conséquences de l'impact de la loi « Ingérences étrangères » sur le budget de la HATVP.

En outre, la HATVP a identifié plusieurs pistes de renforcement du dispositif, qui n'ont pas été intégrées à la loi « Ingérences étrangères », mais qu'il est utile de garder à l'esprit.

La Haute autorité propose ainsi notamment :

- l'instauration d'un pouvoir d'audition et la création d'un délit d'entrave à la mission de la Haute Autorité en plus du possible pouvoir de communication de tout document utile prévu au futur article 18-14 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique ;

- des obligations déontologiques pour les personnes tenues de s'inscrire sur le nouveau registre, identiques à celles applicables aux représentants d'intérêts aux termes de l'article 18-5 de la loi de 2013. Une reprise de ces obligations aurait semblé plus pertinente ;

- l'inclusion parmi les collectivités visées à l'article 18-12-1, des membres des instances exécutives et délibérantes des collectivités à statut particulier d'outre-mer que constituent la Nouvelle-Calédonie et la Polynésie française, qui ne sont pas couvertes par la proposition de loi alors que le risque d'ingérence étrangère peut y être sensible.

La HATVP préconise également que lui soit octroyé d'un pouvoir de sanction administrative en cas de non-dépôt ou de retard dans le dépôt des déclarations. Il convient cependant de relever que la commission des lois du Sénat, saisie du texte, a expressément écarté cette solution tout en faisant

¹ [Rapport n° 2704 \(Assemblée nationale – seizième législature\) et n° 646 \(Sénat – 2023-2024\)](#) fait par Sacha Houlié et Agnès Canayer au nom de la commission mixte paritaire chargée de proposer un texte sur les dispositions restant en discussion de la proposition de loi visant à prévenir les ingérences étrangères en France, déposé le 30 mai 2024.

adopter dans le texte un dispositif d'astreinte qui figure bien dans la loi adoptée.

Pour mémoire, cette loi prévoit la remise d'un rapport au Parlement d'un rapport sur l'état de la menace en 2025, année d'entrée en vigueur du dispositif puis tous les deux ans. À l'occasion de la deuxième remise de ce rapport en 2027, un bilan de sa mise en œuvre après deux ans d'existence pourra être tiré

Recommandation n° 32 : Tirer les conséquences, dans le projet de loi de finances pour 2025, de l'impact de la mise en œuvre de la loi « Ingérences étrangères » sur le budget de la Haute autorité pour la transparence de la vie publique, au regard des nouvelles missions qui lui sont confiées.

Recommandation n° 33 : Intégrer, dans le rapport au Parlement sur l'état de la menace liée aux ingérences étrangères prévu par la loi « Ingérences étrangères », un premier bilan du fonctionnement de la mise en œuvre du dispositif de contrôle des représentants intérêts agissant pour le compte de mandants étrangers présentant, le cas échéant, les limites rencontrées par la Haute autorité pour la transparence de la vie publique.

b) Veiller à défendre, au niveau européen, un haut niveau d'exigence en matière d'encadrement des représentants d'intérêts agissant pour le compte d'un mandant étranger

La commission d'enquête alerte sur le fait que préservation des équilibres du nouveau régime français de contrôle des représentants d'intérêts agissant pour le compte d'un mandant étranger dépendra en partie du contenu de la législation européenne à venir en la matière.

En effet, le principal texte du paquet législatif « défense de la démocratie » encore en cours de discussion au sein de l'Union européenne est la directive établissant des exigences harmonisées dans le marché intérieur en matière de transparence de la représentation d'intérêts exercée pour le compte de pays tiers. La Commission européenne avait introduit cette proposition de directive en réaction à l'affaire dite du « Qatargate » au sein du Parlement européen. L'objet principal du texte est de renforcer la transparence de ce secteur en prévoyant l'inscription des entités exerçant des activités de représentation d'intérêts pour le compte

Lors du déplacement effectué à Bruxelles par une délégation de la commission d'enquête, le représentant permanent de la France auprès de

l'Union européenne, M. Philippe Léglise-Costa, a souligné que le champ de la proposition de directive, qui concerne uniquement les activités de prestation de services de représentation d'intérêts, serait plus restrictif que celui prévu par la loi « Ingérences étrangères ».

Surtout, la proposition de directive prévoit, en l'état actuel de sa rédaction, un niveau d'harmonisation maximal, ce qui signifie que les États membres, dans la transposition de la directive en droit national, doivent introduire des règles respectant les normes minimales et maximales prévues par la directive. Un niveau d'exigence plus élevé en droit interne sur l'encadrement des représentants d'intérêts agissant pour le compte d'entités étrangères pourrait donc se trouver en contrariété avec le droit de l'Union européenne.

Pour cette raison, la France devra veiller, au cours des négociations sur le paquet « défense de la démocratie », à ce que la directive encadrant la représentation d'intérêts exercée pour le compte de pays tiers prévoit un niveau d'exigence comparable à celui prévu par la loi « Ingérences étrangères »

Recommandation n° 34 : Défendre, au niveau européen dans le cadre de la discussion du paquet « défense de la démocratie », un niveau d'exigence en matière de transparence des activités de représentation d'intérêts exercées depuis l'étranger comparable à celui prévu par la loi « Ingérences étrangères ».

3. Mieux contrôler les risques liés au plus hauts responsables politiques

Lors de son audition devant la commission d'enquête, le ministre de l'intérieur, Gérald Darmanin, s'est étonné du **faible niveau de contrôle préalable à la nomination des ministres** au regard de la problématique des influences étrangères : « *J'ai toujours été étonné que les ministres ne suivent pas d'entretien d'accréditation ni de confidentialité. Ceux qui disposent le plus d'éléments secrets sont les ministres eux-mêmes, qui sont le réceptacle de l'intégralité des notes de renseignement et des échanges oraux avec leurs services. Or pour ma part, je n'ai pas passé d'entretien, d'accréditation, contrairement à mon directeur de cabinet, mon secrétaire ou mon chauffeur. (...) Un ministre reste un homme ou une femme, avec ses propres faiblesses possibles et ses propres liens, mais n'est même pas tenu à effectuer de déclaration sur l'honneur. Un tel dispositif pourrait être intéressant dans une grande démocratie comme la nôtre.* »

La commission d'enquête ne peut que souscrire à cette analyse et considère qu'un tel examen pourrait constituer une bonne pratique préalablement à la nomination de certains ministres particulièrement exposés, sans que celle-ci ne fasse obstacle au pouvoir de nomination des membres du Gouvernement par le Président de la République, tirée de l'article 8 de la Constitution.

Il relève à cet égard que depuis l'entrée en vigueur de la loi du 11 octobre 2013 relative à la transparence de la vie publique¹, les ministres sont déjà soumis à certaines exigences en matière de transparence financière, avec des obligations déclaratives à accomplir dans les deux mois qui suivent leur nomination. La pratique veut déjà que l'article 8-1 de la loi précitée, issue de la loi du 15 septembre 2017 pour la confiance dans la vie politique², les ministres pressentis fassent l'objet de contrôles concernant leur situation fiscale, leurs éventuels conflits d'intérêts ou encore leur casier judiciaire.

Cette pratique date de l'affaire « Cahuzac ». La commission d'enquête plaide pour que l'on se dote de procédures de cette nature pour se prémunir d'une potentielle nouvelle « affaire » liée à une ingérence étrangère.

Recommandation n° 35 : Conduire des enquêtes auprès des ministres « pressentis » pour s'assurer de l'absence d'exposition à des influences étrangères.

4. Encourager un renforcement les règles déontologiques applicables aux amendements parlementaires

En cohérence avec l'approche proposée, selon laquelle chacun doit être acteur de sa protection et de celle des autres vis-à-vis des influences étrangères malveillantes, la commission d'enquête considère que les parlementaires eux-mêmes doivent faire preuve d'exemplarité à cet égard.

Deux ministres auditionnés par la commission d'enquête ont relevé publiquement les interrogations soulevées par certains amendements ou questions de parlementaires, en ce qu'ils entreraient en résonnance avec des opérations d'influence étrangères plus larges.

Le ministre de l'intérieur et des outre-mer, Gérald Darmanin, a ainsi déclaré : « *j'ai eu la responsabilité de plusieurs services de renseignement, et il m'est arrivé de recevoir des notes détaillant des stratégies d'influence et d'entendre des*

¹ Loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique.

² Loi n° 2017-1339 du 15 septembre 2017 pour la confiance dans la vie politique.

questions parlementaires sur ces mêmes sujets trois semaines après dans les hémicycles... »¹.

De même, le ministre des armées, Sébastien Lecornu, a également déclaré : « *en matière de manipulation et d'ingérences étrangères les parlementaires sont des cibles de choix. À cet égard, certains débats parlementaires, voire certains amendements, peuvent surprendre, mais je n'en dirai pas plus* »².

À cet égard, la commission d'enquête considère que le « sourçage » des amendements, dès lors qu'ils sont issus de représentants d'intérêts agissant pour le compte d'un mandant étranger ou de tout autre acteur susceptible à l'égard duquel il est possible de soupçonner un objectif d'influence en lien avec des intérêts étrangers, devrait être largement encouragé au sein des assemblées. Le « sourçage » des questions écrites, orales, ou des questions au Gouvernement serait également souhaitable.

Un récent rapport de Sylvain Waserman défend résolument l'approche du « sourçage » (ou « *sourcing* »). : « *Le “sourcing” des amendements provenant des représentants d'intérêts, autrement dit l'expression en toute transparence de l'origine de l'amendement porté par un parlementaire lorsque celui-ci a été proposé par un lobby et/ou élaboré avec lui. Tout parlementaire est libre de porter l'amendement qu'il souhaite, même s'il s'agit de la reprise telle qu'elle d'une proposition d'un représentant d'intérêts, et la pratique du “sourcing” ne limite en rien cette liberté. Toutefois, elle induit deux types de conséquences pour le parlementaire : être probablement plus vigilant sur les motivations et l'acceptabilité de la proposition formulée par le représentant d'intérêts et le cas échéant, rencontrer d'autres acteurs du secteur pour “contrebancer” cet avis en cas de doute. Cette pratique c'est aussi pour les parlementaires faire preuve d'une certaine “honnêteté intellectuelle” : celle de citer ses sources et de l'assumer pleinement* »³.

Pour mémoire, le guide déontologique du Sénat mentionne déjà cette faculté s'agissant des amendements : « *le Sénateur peut préciser dans l'objet de son amendement qu'il a été travaillé avec un représentant d'intérêts (« sourçage »). Il s'agit d'une faculté, à la discrétion du Sénateur, qui exerce librement son droit d'amendement garanti par l'article 44 de la Constitution* »⁴

S'agissant d'amendements travaillés avec des personnes à l'égard duquel il est possible de soupçonner un objectif d'influence en lien avec des intérêts étrangers, la commission d'enquête considère que chaque parlementaire devrait se donner pour obligation de sourcer son amendement.

¹ [Audition](#) du 28 mai 2024.

² [Audition](#) du 25 juin 2024.

³ Sylvain Waserman, [Propositions pour un lobbying plus responsable et transparent](#), Janvier 2021

⁴ [Guide déontologique du Sénat](#) 2023.

Recommandation n° 36 : Encourager résolument en tant que bonne pratique le « sourçage » des amendements et questions parlementaires lorsqu'ils présentent un lien avec une possible influence étrangère.

C. POURSUIVRE LE RENFORCEMENT DE LA PROTECTION DE L'UNIVERSITÉ ET DE LA RECHERCHE FACE AUX OPÉRATIONS D'INFLUENCE

Eu égard à son exposition aux opérations d'influences étrangères malveillantes, le secteur de l'enseignement supérieur et de la recherche est appelé à constituer un axe majeur de la stratégie appelée de ses vœux par la commission d'enquête.

Cette stratégie doit d'abord permettre, comme cela a été évoqué au I de la présente partie, de **mieux structurer les dispositifs de détection des menaces au sein des établissements**, ce qui passe par une poursuite du renforcement du service de défense et de sécurité (SDS) ainsi que du réseau des fonctionnaires de sécurité et de défense, une meilleure adaptation des outils, tels que la cellule ministérielle de veille et d'alerte (CMVA) aux menaces liées aux influences étrangères, et surtout la formalisation de lignes directrices pour la mise en œuvre de procédures harmonisées de détection au sein des établissements, dont l'application opérationnelle relèverait de la compétence du chef d'établissement. **La commission d'enquête considère en outre que cette stratégie doit s'efforcer d'inclure au maximum, avec des moyens adaptés, les établissements d'enseignement supérieur et de recherche privés.**

Par ailleurs, le ministère doit s'attacher à **poursuivre la mise en œuvre des recommandations du « rapport Gattolin »¹**, dont l'état d'application a été analysé supra (voir *Deuxième partie, III, C*) et le détail annexé au présent rapport.

La commission d'enquête souligne en particulier la nécessité de progresser sur les quatre points suivants.

En premier lieu, une meilleure protection des sciences humaines et sociales, qui constituent une cible privilégiée des opérations d'influences

¹ [Rapport d'information n° 873 \(2020-2021\)](#) fait par André Gattolin au nom de la mission d'information du Sénat sur les influences étrangères extra-européennes dans le monde universitaire et académique français et leurs incidences, déposé le 29 septembre 2021.

étrangères est nécessaires. Ne pas le faire serait méconnaître la nature réelle de cette menace.

L'atteinte de cet objectif peut notamment passer par une poursuite de l'élargissement du dispositif de protection du potentiel scientifique et technique de la Nation (PPST).

Dans ses réponses au questionnaire du rapporteur, le Haut fonctionnaire de défense et de sécurité (HFDS) du ministère a indiqué que le « *le SDS mène, en interne, des réflexions ayant pour objectif de mieux protéger les travaux de recherche les plus sensibles en sciences, au-delà du dispositif PPST. Il s'agirait, grâce à un groupe d'experts, d'analyser plus systématiquement le contenu des travaux menés dans certaines matières stratégiques afin d'évaluer leur criticité (travaux sur les services de renseignement, sur les capacités militaires, etc.) et de réfléchir à des possibilités de protection plus accessibles que celles uniquement permises par la classification au titre du secret de la défense nationale* », telles que le PPST. Ces réflexions méritent également d'être poursuivies.

En deuxième lieu, il convient de poursuivre le renforcement du contrôle des projets d'accords internationaux passés par les universités.

Les exigences de transmissions diligentes pour examen aux ministères compétents sur le fondement de l'article L. 123-7-1 du code de l'éducation doivent être réaffirmés. Le délai d'un mois prévu par cet article devrait être porté à trois mois pour laisser davantage de temps d'expertise au ministère de l'enseignement supérieur et de la recherche.

Les travaux annoncés visant à instaurer, par voie réglementaire, une obligation de saisine pour avis sur les projets de coopération internationale en cas d'implication d'une unité de recherche protégée par le PPST à peine de contravention doivent être menés à leur terme.

Enfin, il conviendrait d'élargir le champ du dispositif de transmission en modifiant l'article L. 123-7-1 précité de façon à prévoir que les accords de recherche passés avec les filiales françaises des entreprises étrangères extra-européennes soient soumis systématiquement à la procédure d'examen des projets d'accord par le ministère.

En troisième lieu, il est nécessaire d'instaurer un régime de transparence sur les financements et les liens d'intérêts extra-européens des chercheurs.

Le cadre aujourd'hui prévu à l'article 411-5 du code de la recherche est à ce jour trop restrictif puisqu'il se limite aux expertises réalisées auprès du Parlement ou des pouvoirs publics constitutionnels.

Le HFDS a indiqué à cet égard qu'un groupe de travail, piloté par le SGDSN avait été constitué et travaille à pouvoir instaurer, de manière effective, une exigence la déclaration par les candidats de leurs éventuels conflits d'intérêts dans les demandes d'accès aux zones à régime restrictif

(ZRR). Cette initiative doit aller de pair avec l'élargissement du dispositif PPST, et partant des ZRR, à la protection des sciences humaines et sociales.

Enfin, en quatrième lieu, il fautachever la mise en œuvre de la recommandation du rapport tendant à prévoir un dispositif de transparence sur les financements étrangers octroyés aux laboratoires d'idées (*think tanks*) et aux établissements d'enseignement supérieur et de recherche privés.

La récente loi « Ingérences étrangères » a bien institué un dispositif de transparence s'agissant des financements étrangers perçus par les laboratoires d'idées, qui serait géré par la HATVP.

Il convient donc de concevoir un dispositif d'inspiration similaire, qui pourrait être géré par le SDS du ministère, s'agissant des établissements privés. Une telle évolution, qui implique la mise en œuvre de procédures déclaratives et le cas échéant par des sanctions pénales en cas de non-respect, passerait également par une modification législative.

En sus de l'application des recommandations du rapport Gattolin, la commission d'enquête propose, suite à l'alerte faite sur le sujet par la ministre de l'enseignement Supérieur et de la recherche lors de son audition, à mieux encadrer les bourses à financement étatique ou para-étatique – ainsi celles proposées par le *China Scholarship Council*, s'agissant desquelles il est documenté que les bénéficiaires doivent rendre compte à l'ambassade de Chine ou à ses proxys.

Recommandation n° 37 : Mener un travail de structuration des dispositifs de détection des menaces liées aux influences étrangères au sein des établissements d'enseignement supérieur et de recherche piloté au niveau ministériel, en incluant les établissements privés.

Recommandation n° 38 : Poursuivre la mise en œuvre des recommandations du « rapport Gattolin », notamment en matière de la protection des sciences humaines et sociales, de contrôle des accords internationaux, et de transparence sur les liens d'intérêts des chercheurs ainsi que sur les financements extra-européens des établissements privés.

Recommandation n° 39 : Prévoir une procédure d'encadrement systématique des bourses à financement étatique ou para-étatique.

D. MAINTENIR UN NIVEAU DE VIGILANCE ÉLEVÉ À L'ÉGARD DES ENJEUX LIÉS AU FINANCEMENT DES CULTES

Comme cela a été montré plus haut (voir *Deuxième partie, III, E*), le financement étranger des cultes est soumis à une obligation déclarative depuis la loi du 24 août 2021 confortant le respect des principes de la République dite (loi CRPR)¹, dont le bilan est jugé plutôt satisfaisant. Le régime de financement des écoles privées hors contrat a également été renforcé.

Cependant, il est impératif que les services de renseignement, en particulier la DGSI et Tracfin, ne baissent pas la garde, compte tenu du risque important d'ingérence étrangère, en particulier d'inspiration islamiste.

Plusieurs pistes peuvent être envisagées pour consolider le dispositif.

Premièrement, le système déclaratif pourrait être affiné, notamment de façon à être en mesure de déterminer la nationalité du financeur (outre son pays d'origine) ou si le financeur est un État.

Cependant, d'après plusieurs acteurs spécialisés auditionnés par le rapporteur, les dernières traces de financement étatique de mosquées, notamment en provenance de l'Arabie Saoudite et du Qatar, datent de 2019, soit avant même l'adoption de la loi CRPR.

Ce constat n'exclut pas de maintenir une vigilance sur les financements privés, qui peuvent être assortis de buts politiques.

En outre, comme cela a été relevé *supra*, la délégation parlementaire au renseignement², dans un rapport récent, a identifié plusieurs points de vulnérabilités dans le régime juridique issu de la loi CRPR :

- son dispositif relatif à l'obligation de déclaration d'intention d'aliéner les locaux cultuels au profit de personnes étrangères ne prend pas en compte les terrains non bâtis. Or, selon la DPR, « de nombreuses associations poursuivent des projets d'acquisition de terrains afin d'y construire des centres culturels ou des mosquées ». Pour combler cette lacune, une solution pourrait consister à modifier les documents nécessaires à l'instruction d'un permis de construire d'un lieu de culte et d'inclure dans les documents exigés le plan de financement y afférent, comme l'a proposé le sénateur Hervé Maurey dans un rapport publié le 17 mars 2015³ ;

- cette loi n'aborderait pas la question de la transparence financière des dons et l'appel à la générosité du public, même s'il doit à cet égard être souligné à cet égard que la réforme du régime applicable aux cagnottes en

¹ Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République.

² [Rapport public n° 1454 \(Assemblée nationale seizième législature\) / n° 810 – \(Sénat 2022-2023\)](#) fait au nom de la délégation parlementaire au renseignement, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023, déposé le 29 juin 2023.

³ [Rapport d'information n° 345 \(2014-2015\)](#) fait par Hervé Maurey au nom de la délégation aux collectivités territoriales et à la décentralisation du Sénat sur le financement des lieux de culte, déposé le 17 mars 2015.

ligne (voir (voir *Deuxième partie, III, E*) répond au moins en partie à cet enjeu. Il convient cependant à cet égard d'aller plus loin en supprimant la limite aux prérogatives de contrôle de Tracfin qui reste posée en l'état du droit à l'article L. 561-2-3 du code monétaire et financier. Une mesure en ce sens a récemment été adoptée par le Sénat à l'initiative de Nathalie Goulet dans le cadre de l'examen en première lecture de la proposition de loi instituant des mesures judiciaires de sûreté applicables aux condamnés terroristes et renforçant la lutte antiterroriste¹ ;

- cette loi ne prévoit pas de dispositif spécifique pour contrecarrer le recours excessif aux sociétés civiles immobilières pour financer et soutenir les associations exerçant le culte. Or, si la loi du 9 décembre 1905 concernant la séparation des Églises et de l'État précise que ces associations peuvent détenir des biens immobiliers lorsque cette détention est en lien avec leur objectif social, il apparaît selon la DPR que nombre d'associations cultuelles ne peuvent justifier d'un tel lien. Il convient à cet égard de renforcer les obligations financières des associations, en leur imposant de détailler, dans le cadre de l'état séparé annexé à leur compte annuel qu'elles doivent tenir en application de l'article 4-2 de la loi n° 87-571 du 23 juillet 1987 sur le développement du mécénat, les parts de sociétés civiles immobilières cédées par un État étranger, par une personne morale étrangère ou par tout dispositif juridique de droit étranger. Là encore, une mesure en ce sens a récemment été adoptée par le Sénat à l'initiative de Nathalie Goulet dans le cadre de l'examen en première lecture de la même proposition de loi instituant des mesures judiciaires de sûreté applicables aux condamnés terroristes.

Comme cela a également été évoqué dans le présent rapport, (voir *Première partie, III*), une mission sur l'islamisme politique et la mouvance des Frères musulmans a été confié en mai 2024 par les ministres de l'intérieur et des affaires étrangères à deux hauts fonctionnaires, l'ambassadeur François Gouyette et le préfet Pascal Courtade. Cette mission, qui doit faire un état des lieux de la menace, en particulier à l'aune du risque d'ingérence étrangère, pourrait être amenée à découvrir de nouveaux points de fuite dans le dispositif.

...

Recommandation n° 40 : Combler les lacunes du cadre juridique issu de la loi du 24 août 2021 confortant les principes de la République en matière de contrôle du financement étranger des cultes.

¹ [Amendement n° 11](#) déposé sur le texte de la commission n° 259 (2023-2024) au stade de la première lecture au Sénat et intégré à l'article 8 ter du texte n° 59 (2023-2024) adopté par le Sénat le 30 janvier 2024.

IV. TROISIÈME CERCLE : POSER COLLECTIVEMENT LES FONDATIONS D'UNE VÉRITABLE RÉSILIENCE DE LA SOCIÉTÉ

A. FINLANDE, ESTONIE ET TAÏWAN : DES EXEMPLES ÉTRANGERS DE RÉSILIENCE COLLECTIVE

L'histoire de ces trois pays est révélatrice d'une culture de confrontation à un adversaire démesuré par la taille et la population (la Russie face à la Finlande et l'Estonie ; la Chine face à Taïwan) et omniprésent dans la mémoire collective des populations par le souvenir de guerres ou l'expérience de confrontations en cours.

Certains traits d'organisation de la lutte contre les influences et ingérences étrangères sont spécifiques à la culture et à l'organisation locales des services publics. Néanmoins plusieurs de leurs caractéristiques méritent d'être citées en exemple :

- la défense globale et l'éducation aux médias pour ce qui concerne le modèle nordique et balte ;
- le principe de réactivité « 2+2+2 » taïwanais : 2 heures, 2 images, 200 mots.

1. Défense globale et éducation aux médias : le modèle nordique et balte de résilience

a) L'exemple finlandais de défense globale fondé sur l'organisation de la sécurité des approvisionnements

Du fait de sa géographie, de son climat et de sa dépendance aux importations d'énergies et de biens, le modèle de résilience de la société finlandaise s'appuie principalement sur un système de sécurité des approvisionnements, de tous ordres (énergie, nourriture, médicaments, matières premières, etc.), géré par une agence intitulée *National Emergency Supply Agency* (NES) dépendant du ministère de l'économie.

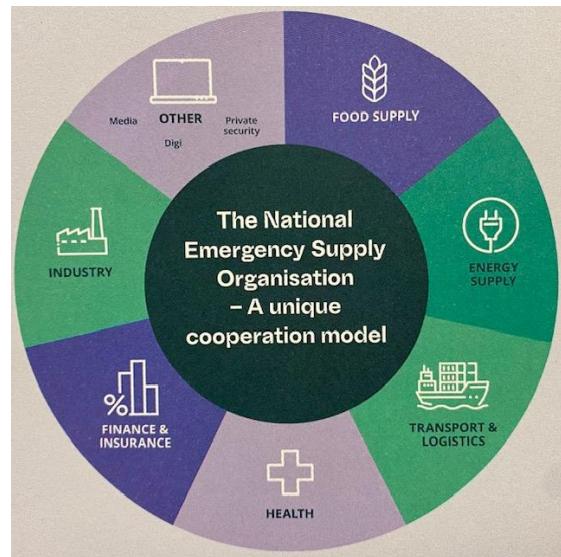
Le crédo de cette organisation est qu'elle ne repose pas prioritairement sur les ministères régaliens comme c'est le cas en France mais au contraire sur l'ensemble du corps social dont les services de l'État ne sont qu'une partie. L'objectif de la stratégie de sécurité de la société est éclairant sur l'approche globale mise en œuvre : elle vise à sécuriser les fonctions vitales de la société par un effort conjoint des autorités, des entreprises, des associations et des individus.

Dans cette optique, la sécurité numérique et celle de l'information sont intégrées dans le même circuit d'alerte et de surveillance que la sécurité des approvisionnements en énergie eau et nourriture, des transports, et de la production industrielle. Le credo de ce modèle repose sur la sensibilisation de l'ensemble des acteurs publics et privés sur les thématiques d'influences et

d'ingérences étrangères, chaque organisation et individu partageant un même interlocuteur, la NESPA.

Le modèle de défense globale finlandais s'appuie sur l'organisation de la sécurité des approvisionnements pour traiter la question des influences et ingérences étrangères en matière cyber et informationnelle.

Source : National Emergency Supply Agency

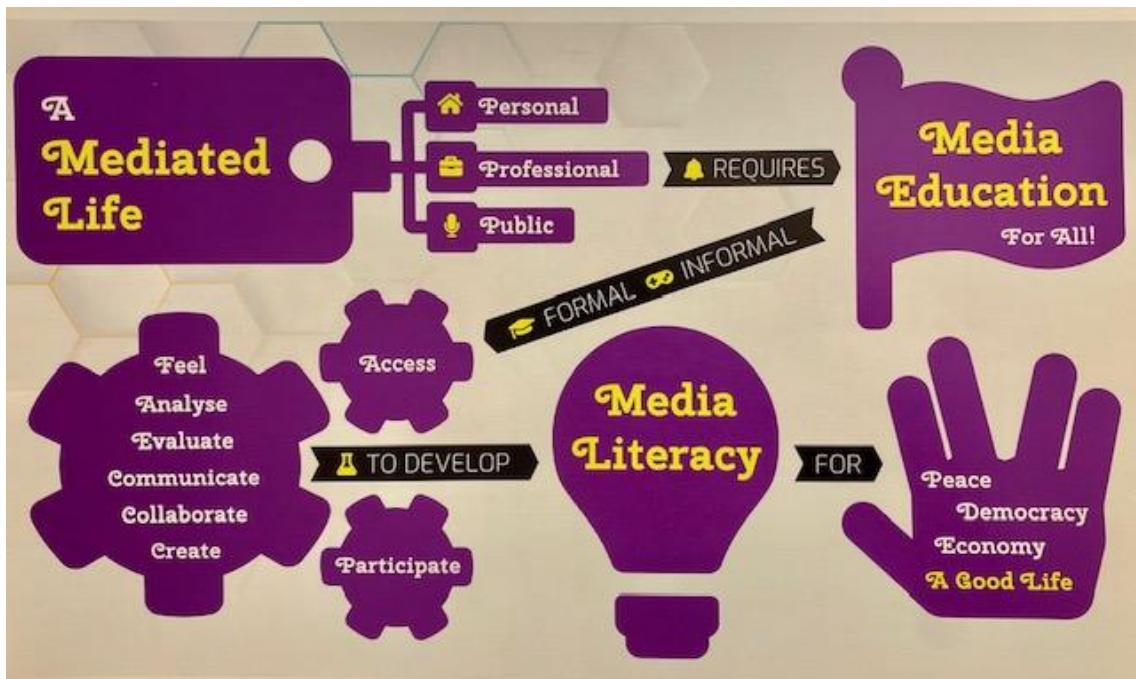


b) L'éducation aux médias : développer l'esprit critique à tous les âges de la vie

L'**éducation aux médias** relève de l'Institut national de l'audiovisuel (KAVI) qui dispose d'un service dédié à cette politique. Celle-ci est présentée comme une **garantie de la paix et de la démocratie** et dispose de relais dans les services publics pour toucher les habitants à tous les âges de la vie, les écoliers comme les personnes âgées. Depuis 2017, la Finlande est classée en tête de l'indice de connaissance médiatique et de résilience face à la désinformation. De fait, le pays connaît également un taux élevé de confiance dans ses institutions et ses médias (lesquels ne cultivent pas le journalisme d'opinion et se cantonne à une presse d'information dans la culture de consensus du pays).

Le but poursuivi de la politique d'éducation aux médias est celui de **cultiver l'esprit critique**. À cet effet, une politique nationale d'éducation aux médias mobilise **une centaine de partenaires et toutes les bibliothèques** du pays. Ainsi, les établissements scolaires de la maternelle au lycée sont chargés de décliner des lignes directrices d'apprentissage du codage informatique, d'utilisation des outils numériques et d'analyse critiques des contenus médiatiques. Le réseau des bibliothèques a vocation à sensibiliser les personnes âgées. Dans l'intervalle, les entreprises, organisations professionnelles et associations partenaires suivent les actifs.

Politique nationale d'éducation aux médias en Finlande



Source : KAVI

c) La stratégie estonienne « 4+1 » de défense psychologique et de communication stratégique

L'Estonie partage également une frontière commune avec la Russie et partage avec la Finlande la particularité de conserver un service national pour la majeure partie de la population masculine et une réserve opérationnelle sensible aux messages de sensibilisation aux menaces étrangères.

Comme en Finlande, **le modèle de sensibilisation aux menaces hybrides est global** à ceci près que le pays, peuplé de seulement 1 million d'habitants, n'a pas les moyens de disposer de structures dédiées, le pilotage de la politique étant assuré par les services du Premier ministre.

La stratégie nationale de sécurité fait trois constats face aux opérations russes de désinformation :

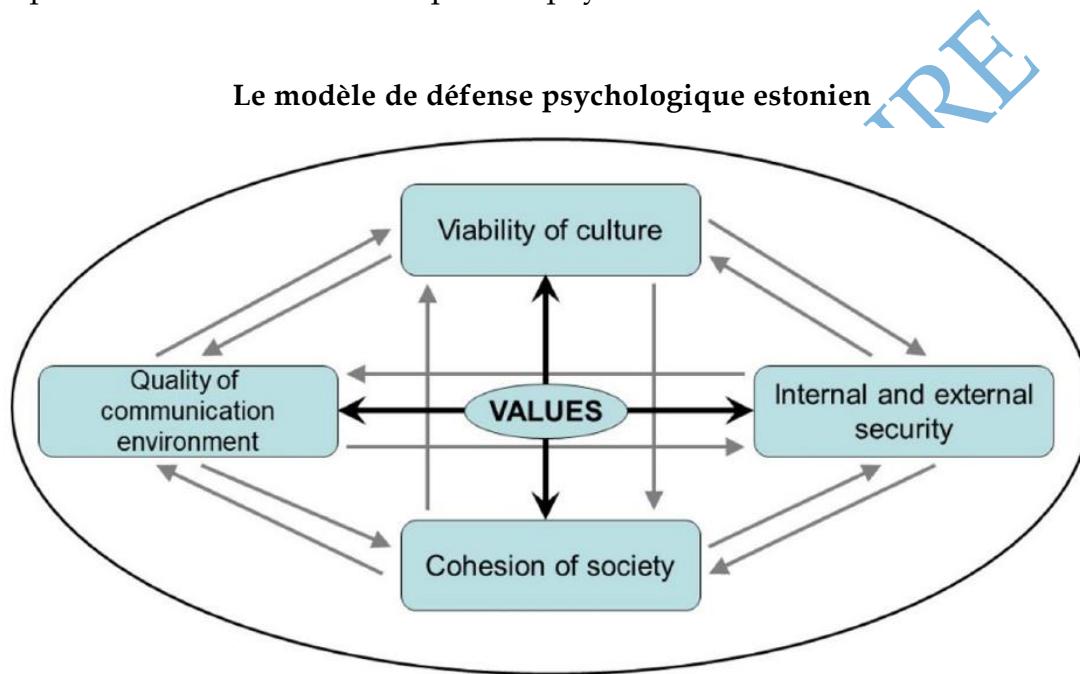
- il n'y a aucun moyen de contrôler ou d'agir sur l'information diffusée par Moscou, donc inutile d'y consacrer des moyens ;

- une fois la fausse information diffusée, son audience restera toujours supérieure à celle de la rectification. La démythification (*debunking*) ne suffit pas ;

- le moyen d'action privilégié de la politique publique estonienne reste l'éducation aux médias et la sensibilisation de la population.

La conclusion de ce triple constat est qu'il faut privilégier l'information et la communication pour « occuper le terrain ». Une position purement défensive conduirait à être perpétuellement en retard.

Aussi, la **stratégie dite « 4+1 »** mise en œuvre (mais non publiée) repose sur **l'articulation entre la communication stratégique et la défense psychologique**. Elle doit son appellation aux caractéristiques suivantes. Quatre critères de communication stratégique sont pris en compte (vitalité de la culture, sécurité interne et externe, cohésion de la société et qualité des moyens de communication) autour d'un pivot incontournable qui doit être le respect des valeurs démocratiques du pays.



Source : *Psychological Defence and Cyber Security: Two Integral Parts of Estonia's Comprehensive Approach for Countering Hybrid Threats* (Dr. Ivo Juurvee, Head of Security & Resilience Programme)

Ce modèle se base sur le principe de la communication stratégique plutôt que sur celui de la contre-influence, en s'appuyant sur un niveau de confiance fort des individus dans les valeurs et les institutions du pays.

2. Le principe de réactivité « 2+2+2 » taïwanais : 2 heures, 2 images, 200 mots

Face aux intrusions de navires et d'aéronefs chinois, la doctrine de défense de l'île repose sur une permanence opérationnelle constante de ses forces conventionnelles. Il en est de même dans le domaine des attaques cyber et informationnelles dont la responsabilité incombe à une agence unique. Celle-ci est chargé de la mise en œuvre de la stratégie de lutte contre la désinformation selon le principe d'une réponse systématique en 2 heures, 2 images et 200 mots.

Ce niveau d'industrialisation des opérations de contre-influence diffèrent donc très sensiblement de la doctrine française, quoique celle-ci s'en rapproche dans les cas de signalement de faux sites internet officiels, et balte.

L'intégration des moyens cyber et informationnels peuvent faciliter le traitement de la chaîne de détection, caractérisation et attribution, tout comme la prévisibilité des thématiques d'attaques chinoises.

Néanmoins, comme on l'a vu dans la dénonciation de certaines fausses informations, la rapidité de rédaction s'avère primordiale (faux charnier de Gossi, faux cercueils de soldats français, etc. – voir *Première partie, IV*), l'exemple taïwanais reste valable à l'échelle française à condition d'ouvrir Viginum et le dispositif régalien de coordination à un partage en réseau avec l'ensemble de la communauté des médias et des vérificateurs d'information.

B. AU TRAVERS D'UNE APPROCHE FONDÉE SUR LA RÉSILIENCE DE LA SOCIÉTÉ FRANÇAISE, CITOYENS ET RESPONSABLES PUBLICS DOIVENT ÊTRE PLUS LARGEMENT SENSIBILISÉS

1. Soutenir la société civile dans la prise de conscience de l'impératif de sécurité informationnelle

La prise de conscience, par la société civile, de la menace s'est érigée en priorité des politiques de lutte contre des opérations d'influence malveillantes. À cet égard, les actions de divulgation et d'attribution, notamment fondées sur les travaux de Viginum, ont permis deux avancées significatives. D'une part, **une meilleure information du public par travail d'exposition et d'explication de la menace**. D'autre part, **l'émergence d'un écosystème de lutte contre les manipulations de l'information**, d'abord fondé sur la transparence des rapports techniques, puis par des échanges entre les différents acteurs concernés, qu'il s'agisse d'associations, de consortiums de journalistes et vérificateurs ou d'organisations non gouvernementales. Ce dernier point doit désormais constituer un levier pour renforcer la prise de conscience de la société civile.

À cet égard, l'évolution des moyens et des missions de Viginum devrait permettre une plus grande mobilisation de ce nouvel écosystème de la lutte contre les manipulations de l'information. Il apparaît ainsi nécessaire de formaliser, au sein du décret du 13 juillet 2021, **une nouvelle fonction de formation et de sensibilisation à la sécurité informationnelle**.

Dans cette logique, l'« *Académie de la lutte contre les manipulations de l'information* » pourrait, en sus de ses activités de formation, **devenir un forum de dialogue et d'échange sur les enjeux de désinformation**. Viginum a déjà initié en 2023 des « *Rencontres et débats autour des manipulations de l'information* », associant chercheurs et journalistes spécialistes intéressés par ces questions, qui pourraient utilement être hébergées et reproduites par l'Académie.

De même, le futur centre d'excellence sur l'intelligence artificielle, visant à renforcer les compétences internes de Viginum dans ce domaine, devrait également être mobilisé pour participer au renforcement de la résilience de la société civile. Des partenariats avec centres de recherche en matière d'intelligence artificielle pourraient être développés. Dans le champ des armées, le Comcyber et la direction générale de l'armement – maîtrise de l'information se sont appuyés sur l'écosystème universitaire rennais pour acquérir de nouveaux instruments de détection et de réaction. Une telle démarche devrait être reproduit à son échelle par Viginum.

Les outils ainsi développés **pourraient être partagés avec l'écosystème des journalistes et vérificateurs de l'information** pour soutenir leurs propres activités d'analyse des campagnes de désinformation. Si les cellules de vérification de l'information utilisent d'ores et déjà l'intelligence artificielle, **les potentialités de ces instruments demeurent encore limitées** comme l'a rappelé Grégoire Lemarchand, rédacteur en chef Investigation numérique à l'AFP : « *En tant que médias, nous essayons de voir comment l'utiliser. C'est déjà en partie le cas : lorsque nous cherchons à tracer une image manipulée sur un moteur de recherches, l'outil dont nous nous servons est une intelligence artificielle. Mais nous nous heurtons aussi à des limites. Nous rêverions tous d'avoir un logiciel capable d'identifier l'authenticité d'une photo ou d'une vidéo. Il va falloir attendre un peu...* »¹. Cette approche collaborative permettrait, de plus, de susciter pour ces médias une alternative aux outils proposés par des entreprises privées et les grandes plateformes numériques.

Dans le prolongement de ces initiatives, déjà envisagées par Viginum, il paraît indispensable d'orienter également ces actions de sensibilisation et de formation vers le secteur privé, encore peu investi face à la menace informationnelle. **Les entreprises constituent pourtant une cible potentielle pour les opérations d'influence.** L'appel au boycott du groupe Carrefour par des internautes chinois en 2008 pour protester contre le soutien de la France au Dalai-Lama constitue un exemple, certes ancien, mais assez représentatif de ce type de manœuvres². À l'époque, le distributeur français avait été accusé par la Chine, sans fondement, de soutenir financièrement le mouvement tibétain. Depuis le développement des plateformes, **les manœuvres informationnelles peuvent prendre la forme de campagnes plus massives de désinformation en ligne** diffusant de manière inauthentique des contenus hostiles à l'entreprise visée. L'usage de techniques de *typosquatting* et l'usurpation de l'identité d'une marque peuvent également être mobilisées.

Pour sensibiliser les entreprises au risque informationnel, les services de l'État et, en premier lieu, Viginum, chef de file en la matière, **doivent intensifier leurs actions d'information du secteur privé**. En prévision des Jeux olympiques et paralympiques de Paris, Viginum a publié un « *Guide*

¹ [Audition](#) du 14 mai 2024.

² France 24, « [Les internautes chinois pour le boycott de carrefour](#) », 16 avril 2008, en ligne, consulté le 11 juillet 2024.

sensibilisation à la menace informationnelle », à destination des entreprises associées à l'organisation de l'évènement¹. Ce document rappelle les différents risques auxquels sont exposées ces sociétés :

- un **risque réputationnel**, pour l'image de l'entreprise ;
- un **risque économique**, pouvant conduire à une dégradation de sa valeur boursière ou un boycott de ses produits ;
- un **risque sécuritaire**, lié aux risques de troubles à l'ordre public pouvant découler de ces attaques informationnelles.

L'initiative de ce guide devrait être élargie à l'ensemble du secteur privé. Un modèle pouvant être suivi en la matière est **celui des « Flash ingérence » de conseil aux entreprises publiés mensuellement par la DGSI**. Cette dernière présente ainsi, selon ses actualités, les risques d'ingérence pouvant affecter les entreprises². Une approche similaire **pourrait être adoptée par Viginum et le SGDSN** et complétée par des sessions de sensibilisation et de conseil auprès de grandes entreprises volontaires. Il convient à cet égard de noter que Viginum s'est déjà doté d'une certaine expertise sur la question, en consacrant l'une de ses opérations permanentes à la veille en matière de potentielles ingérences numériques étrangères ciblant les intérêts économiques, industriels et scientifiques français (voir *Deuxième partie, I*).

Ces actions de formation devraient s'articuler avec celles que prodiguent l'Anssi sur les enjeux de cybersécurité, ou de la DGSI sur les ingérences. À cet égard, il a été porté à la connaissance de la commission d'enquête que de **nombreuses entreprises, en particulier dans des domaines sensibles comme la base industrielle et technologique de défense, sont encore insuffisamment protégées** contre les risques d'intrusion cyber. Le risque cyber, comme exposé supra, **est indirectement relié au sujet de la commission d'enquête**. Pour autant, la commission d'enquête estime que la protection du patrimoine scientifique et technologique français ainsi que du secret de la défense nationale **commanderait une approche plus coercitive sur les obligations applicables aux entreprises « stratégiques » en matière cyber**.

Par ailleurs, **au-delà d'une démarche de sensibilisation et de formation, il importe de structurer une véritable filière de la sécurité informationnelle**. Une telle orientation suivrait l'exemple de l'Anssi qui a entrepris, dans le domaine de la cybersécurité, de soutenir l'émergence d'une véritable filière professionnelle. Pour cela, l'Anssi a développé deux approches :

¹ Viginum, [« Guide de sensibilisation à la menace informationnelle. Écosystème des acteurs économiques associés aux Jeux olympiques et paralympiques de Paris 2024 »](#), mai 2024.

² Par exemple : DGSI, [« Les salons professionnels, sources de vulnérabilité pour les entreprises »](#), Flash ingérence, octobre 2023.

- une démarche directe de formation, au travers du Centre de formation à la sécurité des systèmes d'information (CFSSI), destinée aux agents publics ;

- une démarche plus indirecte, de mise en valeur des métiers et des formations de la cybersécurité. L'Anssi a ainsi créé un label CyberEdu permettant aux étudiants et aux employeurs d'identifier les formations liées au cyber et met à la disposition des enseignants des contenus pédagogiques relatifs à la cybersécurité. L'Agence participe également à la promotion du secteur en publiant des enquêtes sur l'attractivité des métiers de la cybersécurité.

Recommandation n° 41 :Créer, au sein de Viginum, une nouvelle fonction de sensibilisation et de formation à la sécurité informationnelle, y compris en direction des acteurs privés.

2. Sensibiliser plus largement la population face aux risques des influences malveillantes

a) Renforcer l'esprit critique de nos citoyens par une politique ambitieuse en direction de la jeunesse

Le renforcement de la résilience de la population face à la désinformation passe par une montée en puissance des dispositifs de d'éducation aux médias et à l'esprit critique, comme l'a notamment souligné le récent rapport de l'OCDE consacré à la désinformation¹.

Comme indiqué dans le III de la deuxième partie du présent rapport, la France s'est d'ores et déjà dotée d'un dispositif d'éducation aux médias et à l'information. Une circulaire du ministère de l'éducation nationale, en date du 24 janvier 2022, a généralisé l'EMI au sein du cursus scolaire. Pour autant, cette priorité ne s'est pas encore véritablement traduite dans les faits. Les dispositifs d'éducation aux médias reposent sur des initiatives dispersées, encore peu harmonisées.

Pourtant, le Parlement s'était prononcé à de multiples reprises en faveur d'un renforcement des dispositifs d'éducation aux médias et, plus largement à l'éducation des élèves à l'information et au numérique. Dans un rapport d'information de 2018 de Mme Catherine Morin-Desailly, la commission de la culture, de l'éducation, de la communication et du sport du

¹ OCDE, [Les faits sans le faux. Lutter contre la désinformation, renforcer l'intégrité de l'information](#), 2024.

Sénat avait ainsi recommandé de faire de la montée en compétence numérique une grande cause nationale¹. De même, en 2023, une mission flash de la commission des affaires culturelles et de l'éducation de l'Assemblée nationale a proposé de déclarer l'éducation aux médias et à l'information grande cause nationale².

Au-delà de la problématique de sa mise en œuvre, l'éducation aux médias et à l'information n'intègre pas la dimension spécifique des influences étrangères malveillantes, comme indiqué *supra*. Or la désinformation, en particulier sur les réseaux sociaux, est très largement encouragée par des opérations d'influence étrangères.

Comme le relève le chercheur David Colon, « *s'agissant de l'éducation aux médias, celle-ci est aujourd'hui peu financée, peu généralisée et très peu évaluée. Une évaluation concrète de ce qui fonctionne ou non est nécessaire. Cela nécessite de l'investissement public* »³. Il apparaît donc nécessaire de conduire, presque deux ans après la généralisation de l'EMI, une **évaluation exhaustive et approfondie de nos dispositifs d'éducation aux médias et plus largement, de formation à l'esprit critique**. Un tel travail d'évaluation permettrait :

- de déterminer si le modèle d'EMI et à l'éducation à l'esprit critique choisi par la France, à savoir un enseignement distinct des autres matières, doit être préféré à d'autres modèles pratiqués à l'étranger, en particulier en Finlande où l'éducation à l'esprit critique est transversale à l'ensemble des matières ;

- de mesurer l'efficacité de ce type d'enseignement, en particulier s'il est associé à une éducation à l'esprit critique. Le chercheur David Cordonier a, en effet, souligné devant la commission d'enquête le **risque de renforcer la défiance des jeunes au travers de ces enseignements** : « *avant d'implémenter quoi que ce soit dans les écoles ou ailleurs, il faut en tester l'efficacité pour ne pas dépenser de l'argent public en pure perte. Il faut également procéder à des tests pour savoir si l'action déployée n'est pas contre-productive. Un certain nombre de pistes d'études nous permettent aujourd'hui de penser – les résultats n'étant pas encore consolidés – que des formations à l'esprit critique mal conduites rendent les gens complotistes* »⁴.

À l'issue d'un tel travail, le journaliste Gérald Holubowicz estime qu'il serait nécessaire de : « *mettre en place un plan décennal et imaginer sur le temps long une intégration fine de l'éducation aux médias dans l'enseignement scolaire, qui ne soit plus seulement le fait d'intervenants extérieurs ponctuels*.

¹ [Rapport d'information n° 607 \(2017-2018\)](#) fait par Mme Catherine Morin-Desailly au nom de la commission de la culture, de l'éducation et de la communication du Sénat sur la formation à l'heure du numérique, déposé le 27 juin 2018.

² [Communication de la mission flash sur l'éducation critique aux médias, au nom de la commission des affaires culturelles](#), par Mme Violette Spillebout et M. Guillaume Ballard, déposé le 15 février 2023.

³ [Audition](#) du 29 février 2024.

⁴ [Audition](#) du 7 mars 2024.

Il faudrait une structuration pédagogique autour de l'information aux médias, y compris avec une approche technique du numérique »¹. La mise à plat de notre politique d'EMI impliquera nécessairement d'y intégrer une dimension liée aux influences étrangères.

Recommandation n° 42 : Mener une évaluation exhaustive des dispositifs français d'éducation aux médias et plus largement à l'esprit critique pour consacrer l'éducation aux médias et à l'information comme grande cause nationale, en y intégrant une dimension spécifique aux influences étrangères malveillantes.

Une meilleure appréhension des médias et de l'information par la jeunesse **repose également sur un accès à des sources fiables**. Si l'éducation aux médias et à l'information permet d'acquérir les réflexes nécessaires à une meilleure résilience face à la désinformation, **nos jeunes concitoyens peuvent connaître des obstacles économiques dans leur recherche d'information**. L'un des moteurs de plateformes, principale source d'information de la jeunesse, est leur apparente gratuité. Cette forme de concurrence déloyale pourrait être **compensée par un dispositif de soutien financier aux jeunes dans leur relation aux médias**, sous la forme d'un « *Pass Médias* », comme le suggère RSF².

Ce dispositif découlerait du système existant pour le *Pass Culture*. Ce dernier, expérimenté à partir de 2019 puis généralisé et élargi à compter de 2021, **consiste en une application relayant les offres culturelles aux jeunes de 15 à 18 ans**. Ces derniers disposent d'une enveloppe entre 20 et 300 euros, variant selon l'âge, leur permettant de financer ces offres. Dans ce cadre, le *Pass Culture* présente des offres de presse en ligne parmi lesquels *Courrier International*, *ePresse*, *Ouest France*, *Le Télégramme* ou *Vocabule*. **Un plafond de 100 euros est toutefois fixé pour les abonnements en ligne**. Depuis juin 2024, il est désormais possible d'utiliser le *Pass* dans les maisons de la presse.

Pour renforcer le droit à l'information, il pourrait être envisagé de **créer un dispositif distinct du *Pass Culture* pour financer des abonnements presse pour les jeunes à partir de 15 ans** et en repoussant l'âge de sortie du dispositif à 25 ans. *A minima*, il serait souhaitable de supprimer le plafond de 100 euros pour les abonnements à des titres de presse.

Si la commission d'enquête n'a pas pour objet ni pour ambition de formuler des recommandations visant à solutionner la crise économique du

¹ *Audition* du 9 avril 2024.

² RSF, « 30 propositions pour le droit à l'information », *Livre blanc*, 2022.

secteur de la presse écrite, **un tel dispositif contribuerait indéniablement à soutenir le niveau des abonnements à la presse écrite**. En s'appuyant sur les mécanismes de labellisation des médias, il reviendrait à **une forme de « bonus » accordé aux titres de presse** les plus respectueux des exigences déontologiques et de l'objectif de qualité de l'information.

Recommandation n° 43 : Créer un Pass Médias pour les jeunes, sur le modèle du Pass Culture.

En outre, en complément de l'éducation aux médias et à l'information, le renforcement de l'esprit critique au sein de la jeunesse bénéficierait d'un temps réservé au sein de la Journée défense et citoyenneté (JDC). Lors de son audition par la commission d'enquête, **le ministre des armées, Sébastien Lecornu, a ainsi évoqué une potentielle évolution de la JDC vers une « JDC durcie », comprenant une dimension liée aux influences étrangères** : « *j'ai amorcé une transformation profonde de la Journée défense et citoyenneté (JDC), l'ancienne Journée d'appel de préparation à la défense (JAPD), qui aujourd'hui n'a plus grand-chose à voir avec la défense, alors qu'elle est financée par le ministère des armées. Pour cette cible d'âge – 16 ans –, plutôt que de s'éparpiller sur divers sujets, il vaudrait mieux se concentrer sur quelques règles de vigilance numérique et autres qui trouveraient bien leur place dans une « JDC durcie »* »¹. La JDC serait ainsi l'occasion de **présenter aux nouvelles générations un état de la menace et de les former à des « réflexes de résilience » reposant principalement sur des bonnes pratiques numériques et informationnelles**.

Recommandation n° 44 : Intégrer dans la Journée défense et citoyenneté une dimension portant sur les influences étrangères.

Par ailleurs, une association plus opérationnelle de la société civile à l'entrave aux opérations d'influence pourrait être envisagée, sous la forme d'une « réserve ». Cette dernière suivrait le modèle de la réserve de cybersécurité de l'Union européenne, prévu dans le règlement sur la cybersolidarité, en cours d'examen. La réserve permet à des prestataires de confiance d'intervenir en soutien des institutions européennes et des États membres lorsqu'ils font face à des attaques cyber. Le même principe pourrait être mobilisé en droit interne, afin de solliciter, dans le contexte d'une attaque

¹ [Audition](#) du 25 juin 2024.

informationnelle d'ampleur visant le débat public français, des prestataires de confiance, à savoir des organisations non gouvernementales ou des organismes de vérification de l'information.

Ainsi, la commission d'enquête propose de créer une spécialité de la réserve opérationnelle et de la réserve citoyenne de défense et de sécurité dédiée à la fonction d'influence et mobilisable pour la détection et la riposte aux opérations d'influence étrangères.

Recommandation n° 45 : Créer une spécialité de la réserve opérationnelle et de la réserve citoyenne de défense et de sécurité dédiée à la fonction d'influence et mobilisable pour la détection et la riposte aux opérations d'influence étrangères.

b) Associer l'ensemble des responsables publics aux politiques de lutte contre les opérations d'influence

Le « troisième cercle » des politiques de lutte contre les influences malveillantes implique de **mieux associer certains acteurs, jusque-là placées hors du champ de la réponse à ces menaces**. Les responsables publics, regroupant tant les élus que les dirigeants des organismes divers d'administration centrale, **paradoxalement peu au fait des opérations d'influence dont ils sont pourtant une cible fréquente**, devraient donc être davantage formés et informés.

S'agissant des élus locaux, la commission d'enquête fait sienne la recommandation formulée par la délégation parlementaire au renseignement, dans son rapport consacré aux ingérences étrangères¹ et jusque-là non mise en œuvre, **d'organiser des sessions de sensibilisation et de formation des élus locaux, en particulier au lendemain de chaque élection locale**. Ces sessions seraient organisées par le représentant de l'État dans chaque territoire concerné, en lien avec les services territoriaux de sécurité intérieur. Elles devraient tout particulièrement intégrer une dimension consacrée à la commande publique et aux risques d'influence découlant d'investissements économiques ciblés. La vigilance des élus pour alerter les services compétents d'une offre économique suspecte est en effet cruciale, comme l'a souligné le chef de servie du Sisse, Joffrey Célestin-Urbain : « *Le problème n'est réglé que grâce à un réflexe qu'ont les entreprises publiques et les administrations qui gèrent ces marchés sensibles : elles nous consultent en amont de la rédaction des marchés.*

¹ [Rapport public n° 1454 \(seizième législature- Assemblée nationale\) / n° 810 \(2022-2023 – Sénat\)](#) fait par Sacha Houlié au nom de la délégation parlementaire au renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023, déposé le 29 juin 2023.

Ces interventions restent néanmoins très ponctuelles, et souvent liées à des contentieux »¹.

Par ailleurs, dans une réflexion similaire à celle formulée à propos des entreprises *supra*, la commission relève que la sensibilisation des élus aux risques de cybersécurité et, en particulier s’agissant des parlementaires, est encore insuffisamment assurée. Les recommandations de fourniture de matériels informatiques sécurisés, notamment lors des déplacements à l’étranger, telles qu’elles sont pratiquées dans de nombreux pays, devraient être mises en œuvre au niveau du Parlement français. Cette préoccupation devrait être étendue aux présidents des grands exécutifs locaux.

En particulier, l’actualité récente a démontré que les départements et régions d’Outre-mer et les collectivités d’Outre-mer sont particulièrement visés par des opérations de manipulation de l’information et de capture des élites, comme en témoignent les récentes déclarations du groupe d’initiative de Bakou, lors de son congrès des 17 et 18 juillet 2024, accusant l’État français de « colonialisme » et de « torture » en Nouvelle-Calédonie.

Recommandation n° 46 : Sensibiliser les élus sur les enjeux liés aux influences étrangères malveillantes (commande publique, cybersécurité etc.).

Certains responsables publics, présidents d’exécutifs locaux ou dirigeants d’établissements publics, demeurent à l’écart de la lutte contre les opérations d’influence en raison d’un accès limité, du fait du secret de la défense nationale, à des informations concernant directement leur champ de compétences. Le code de la défense dispose en effet que « *sauf exceptions prévues par la loi, nul n'est qualifié pour connaître d'informations et supports classifiés s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin, au regard du catalogue des emplois justifiant une habilitation, établi dans les conditions définies par arrêté du Premier ministre, de les connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission* »². À titre d’exemple, les échanges entre les présidents d’université et les fonctionnaires de sécurité et défense (FSD) placés auprès des établissements d’enseignement supérieur et de recherche ne peuvent aborder certaines informations relatives aux menaces pesant sur le patrimoine scientifique et technologique de la Nation. De même, le président d’un territoire d’Outre-mer, très exposé aux risques d’influences malveillantes, ne peut pas être informé des opérations d’influence qui auraient pu viser sa collectivité.

¹ [Audition](#) du 9 avril 2024.

² Article R. 2311-7 du code de la défense.

À ce titre, il paraîtrait souhaitable d'examiner la possibilité d'habiliter davantage ces responsables publics, en élargissant le catalogue des emplois justifiant une habilitation. Interrogé par la commission d'enquête sur cette possibilité, le ministre de l'intérieur et des Outre-mer, Gérald Darmanin, s'y est montré favorable : « *Il n'est d'ailleurs pas interdit de partager un certain nombre de notes avec des personnes qui ne sont pas des agents de l'État, il suffit de les y habiliter* »¹.

Recommandation n° 47 : Examiner la possibilité d'habiliter au secret de la défense nationale davantage de responsables publics, en particulier les exécutifs locaux et les présidents d'établissements d'enseignement supérieur dans la limite du besoin d'en connaître.

¹ [Audition](#) du 28 mai 2024.

ANNEXE :

ÉTAT D'APPLICATION DES RECOMMANDATIONS DE LA MISSION D'INFORMATION DU SÉNAT SUR LES INFLUENCES ÉTATIQUES EXTRA-EUROPÉENNES DANS LE MONDE UNIVERSITAIRE ET ACADEMIQUE FRANÇAIS ET LEURS INCIDENCES

La mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences¹ a formulé 23 recommandations.

À la demande de la commission d'enquête, le secrétariat général du ministère de l'éducation nationale et de la jeunesse, du ministère de l'enseignement supérieur et de la recherche et du ministère des sports et des jeux Olympiques et Paralympiques a produit un document synthétisant l'état d'application de ces recommandations.

Ce document est reproduit ci-après

¹ [Rapport d'information n° 873 \(2020-2021\)](#) fait par André Gattolin au nom de la mission d'information du Sénat sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences, déposé le 29 septembre 2021.

Etat des lieux de la mise en œuvre des recommandations du rapport de la mission d'information sur les influences établiques extra-européennes dans le monde universitaire et académique français et leurs incidences

Rapport n° 573 (2020-2021) du 29 septembre 2021

Ce document présente un état des lieux de la mise en place des recommandations du rapport de la mission d'information du Sénat sur les influences établiques extra-européennes dans le monde universitaire et académique français et leurs incidences au 31 mai 2024.

Objectif 1 : Élever le sujet des interférences étrangères au rang de priorité politique pour dresser un état des lieux et co-construire avec le monde universitaire des réponses adaptées

1. Dresser un état des lieux des alertes, de la volumétrie des signalements et des mesures prises pour y remédier et évaluer le niveau des influences étrangères dans l'enseignement supérieur et la recherche.

ACTION EN COURS

Le ministère de l'enseignement supérieur et de la recherche (MESR) exerce une vigilance particulière, sans naïveté, sur les opérations d'influences étrangères dans les établissements d'enseignement supérieur. Ses connaissances sont actualisées grâce aux interactions continues entretenues entre le service de défense et de sécurité (SDS), ses homologues, le secrétariat général de la défense et de la sécurité nationale (SGDSN) et les services de renseignement.

La menace est protéiforme et émane principalement d'acteurs établiques identifiés (Chine, Russie, Turquie), mais qu'il n'appartient pas au MESR de recenser. Le MESR n'a pas mandat à faire le lien entre des actions déterminées et des États en particulier. Il contribue toutefois, dans son champ de compétences et en fonction des signaux faibles qu'il repère, aux travaux pilotés par le SGDSN.

Par définition, les actions d'influence étrangère néfaste sont à la fois diffuses, dissimulées et peuvent s'appuyer sur différents vecteurs.

L'administration centrale, dont l'action en la matière est coordonnée par le SDS, comme les fonctionnaires de sécurité et de défense (FSD), ont d'évidentes difficultés à pouvoir percevoir ces vecteurs comme leurs conséquences. Les établissements font état d'une perception de la menace, mais ne parviennent qu'exceptionnellement, faute d'une grille de lecture opérationnelle, à caractériser des incidents dans les faits.

Ce sont notamment des travaux d'enquête (scientifique, policière, de renseignement ou journalistique) qui ont permis de mettre en lumière des manœuvres structurées et manifestes. La persistance d'une zone grise ne permet que rarement de leur adosser une qualification pénale.

L'autonomie de gestion des universités, qui rend le chef d'établissement responsable de la politique de défense et de sécurité, et le principe fondamental de liberté académique font, pour l'heure, obstacle à un recensement et un suivi exhaustifs des situations – compétence de la direction générale de la sécurité intérieure au premier chef.

Des axes de travail permettent déjà d'améliorer la situation :

- Le développement continu du réseau des FSD ;

- La poursuite de la professionnalisation des FSD et la mutualisation des missions entre FSD et référent de la radicalisation ;
- L'ouverture de la cellule ministérielle de veille et d'alerte à l'enseignement supérieur et à la recherche (ESR) ;
- La contribution aux travaux interministériels sur l'utilisation stratégique du droit (« lawfare ») ;
- Le traitement au cas par cas des situations signalées et très sensibles, notamment dans certains établissements.

Cette montée progressive en compétences se traduit par la transmission de signalements de manière très sporadique, sans que celle-ci ne puisse recouvrir un caractère obligatoire. Une vigilance renforcée est portée sur certaines bourses à financement étatique et certaines associations.

2. Constituer un comité scientifique, prenant la forme d'un « observatoire des influences étrangères et de leurs incidences sur l'enseignement supérieur et la recherche » qui associerait universitaires, ministères de l'enseignement supérieur et de la recherche, des affaires étrangères, de l'économie, de l'intérieur et des armées, chargé de dresser un état des lieux, d'en assurer le suivi régulier et de formuler des propositions au Gouvernement.

ACTION NON ENGAGÉE

Sous le pilotage du SGDSN, plusieurs groupes de travail réalisent un important travail de veille, d'anticipation et d'analyse des risques liés aux influences étrangères, que ceux-ci touchent ou non le monde universitaire et la recherche. Ces groupes de travail réunissent l'ensemble des départements ministériels intéressés par ces problématiques – dont le MESR – et les services de renseignement du premier cercle. Au-delà des contributions administratives, ils mobilisent des experts de haut niveau dans les champs thématiques et géographiques qui appellent leur attention.

Le format de ces groupes de travail permet la juste mobilisation des acteurs en fonction de leurs compétences et une mise en perspective stratégique ou opérationnelle efficace des enjeux, en fonction des priorités politiques.

La diversité et la porosité des moyens et des cibles des opérations d'influence étrangère ne rendent pas pertinente une segmentation de l'action interministérielle sur ces problématiques, qu'il est nécessaire d'envisager dans leur ensemble et leur complexité. Au sens du MESR, la création d'un comité ad hoc spécifiquement chargé de l'observation des influences étrangères dans l'écosystème académique français serait superfétatoire.

3. Charger le comité d'élaborer une étude scientifique de référence sur l'état des menaces constatées en France. Ce document, qui ferait l'objet d'un suivi actualisé et d'une analyse des évolutions dynamiques, comporterait une vision globale des menaces extra-européennes et une cartographie des risques à la fois thématiques et géographiques.

ACTION NON ENGAGÉE

Les groupes de travail mentionnés supra élaborent des documents de référence, actualisés et prospectifs, susceptibles de porter sur l'état des menaces constatées en France. Ces travaux sont, pour la majorité d'entre eux, classifiés au titre de la protection du secret de la défense nationale. Il appartiendrait au SGDSN, autorité émettrice, de permettre la diffusion de ces documents aux établissements d'ESR, notamment via les FSD, s'il le jugeait utile.

4. Prévoir la transmission de cette étude et de ses versions actualisées au Parlement. Ses constats pourront faire l'objet d'un débat.

Sans objet.

Objectif 2 : Aider les universités à protéger leurs valeurs de libertés académiques et d'intégrité scientifique dans le respect de leur autonomie

5. Étendre le dispositif de protection du patrimoine scientifique et technique de la Nation (PPST) à l'ensemble des disciplines universitaires, notamment en les adaptant aux enjeux et influences spécifiques aux sciences humaines et sociales qui en sont exclues.

ACTION EN COURS

La réglementation relative à la protection du potentiel scientifique et technique (PPST) de la Nation est fondée sur des dispositions du code pénal et vise à protéger les savoirs, savoir-faire et technologies les plus sensibles des établissements publics et privés localisés sur le territoire national dont le détournement ou la captation pourraient :

- Porter atteinte aux intérêts économiques de la Nation ;
- Renforcer des arsenaux militaires étrangers ou affaiblir les capacités de défense de la Nation ;
- Contribuer à la prolifération des armes de destruction massive et de leurs vecteurs ;
- Être utilisés à des fins terroristes sur le territoire national ou à l'étranger.

Seule une très profonde adaptation, aux contours difficilement définissables, permettrait son application aux domaines classiques des sciences humaines et sociales (droit, sciences politique, histoire, langues, sociologie, etc.) – pour lesquels l'identification et la caractérisation de l'un ou plusieurs des risques définis par l'état actuel de la réglementation est particulièrement complexe.

Toutefois, suite à la parution du décret en Conseil d'État relatif au renforcement de la réglementation PPST (décret n° 2024-480 du 14 mai 2024 portant diverses dispositions relatives à la protection du potentiel scientifique et technique de la Nation), qui entrera en application le 1^{er} janvier 2025, sera publié au cours de l'année 2024 un arrêté modifiant l'arrêté du 8 juillet 2012 relatif à la protection du potentiel scientifique et technique de la Nation. Cet arrêté interministériel, qui fait actuellement l'objet d'une concertation pilotée par le SGDSN, devrait intégrer plusieurs domaines, secteurs et spécialités sensibles relevant des sciences humaines et sociales (SHS) dans la liste des secteurs scientifiques et techniques protégés (SSTP), notamment :

- Les sciences cognitives et neurosciences ;
- Les sciences du langage (linguistique et phonétique générale) ;
- Les psychologie, psychologie clinique, psychologique sociale ;
- Les sciences et techniques des activités physiques et sportives ;
- L'ergonomie.

Par ailleurs, le SDS mène, en interne, des réflexions ayant pour objectif de mieux protéger les travaux de recherche les plus sensibles en sciences, au-delà du dispositif PPST. Il s'agirait, grâce à un groupe d'experts, d'analyser plus systématiquement le contenu des travaux menés dans certaines matières stratégiques afin d'évaluer leur criticité (travaux sur les services de renseignement, sur les capacités militaires, etc.) et de réfléchir à des possibilités de protection plus accessibles que celles uniquement permises par la classification au titre du secret de la défense nationale.

6. Confier au collège de déontologie de l'enseignement supérieur, de la recherche et de l'innovation une mission renforcée d'animation du réseau des déontologues au sein des établissements et à la procédure d'identification.

ACTION MENÉE

Le rapport d'activité 2022 du collège de déontologie de l'enseignement supérieur et de la recherche (dernier en date) souligne un nombre croissant de saisines pour avis (45 en 2022) et, par là même, une structuration du réseau et une meilleure connaissance de son rôle.

7. Assurer sur une base régulière un échange d'informations entre le collège de déontologie et le Haut Fonctionnaire de Défense et de Sécurité (HFDS) du MESRI, sur toute question relative aux influences étrangères menaçant les libertés académiques.

ACTION NON ENGAGÉE

Le SDS dispose d'une expertise propre sur les sujets relatifs aux influences étrangères, largement étoffé par les contributions des services de renseignement, des échanges interministériels et des FSD. Il prend connaissance avec attention des avis du collège de déontologie de l'ESR.

Toutefois, aucun échange régulier n'est assuré entre les deux structures, là où un tel processus présenterait certainement un intérêt au regard des enjeux soulevés par les travaux du collège (intégrité scientifique, conflit d'intérêt, cumul d'activité et liberté d'expression).

8. En lien avec le collège de déontologie, renforcer le service du Haut Fonctionnaire de Défense et de Sécurité (HFDS) et le doter d'une expertise dédiée.

ACTION EN PARTIE ENGAGÉE

Sans lien particulier avec le collège de déontologie de l'ESR (cf. *supra*), le service spécialisé de défense et de sécurité a été renforcé. Son plafond d'emplois a évolué de 29 ETP à 44 ETP entre 2021 et 2024.

Il dispose aujourd'hui de onze experts scientifiques à temps partiel affectés au pôle PPST. Il est en charge, au niveau ministériel, de la coordination de la politique publique en matière de lutte contre les ingérences étrangères à l'université.

9. Constituer un réseau formalisé des fonctionnaires de sécurité et de défense (FSD), afin de leur permettre de bénéficier de l'expertise des services des ministères, d'échanger sur leurs pratiques et de centraliser les signalements.

ACTION MENÉE

Le réseau des FSD des établissements d'ESR existe depuis 2018. Sa structure s'est considérablement renforcée depuis plusieurs années.

Il compte 143 FSD et 69 adjoints, en forte augmentation. Les FSD sont nommés par le HFDS, sur proposition de la gouvernance des établissements. Ils assurent également le rôle de référents de la radicalisation. Ils peuvent avoir un ou des adjoints.

Les FSD exercent dans 72 universités, 39 écoles d'ingénieurs, 20 organismes de recherche, 5 instituts d'études politiques, 2 communautés d'universités et établissements (COMUE), 1 grand établissement (Collège de France), 2 établissements publics administratifs (dont CNOUS), 1 organisme de droit privé spécifique (Institut Pasteur) et 1 groupement d'intérêt public.

Le SDS organise chaque année un séminaire du réseau permettant de poursuivre la sensibilisation des FSD et FSD adjoints aux enjeux de défense et de sécurité, d'actualiser leurs connaissances, de leur permettre de partager leurs expériences.

Une session de formation se tient par ailleurs tous les ans pour les FSD nouvellement nommés (une trentaine de participants sur environ quarante personnes concernées). Tous les champs d'action du service dans les établissements d'ESR leur sont présentés.

La quasi-totalité des FSD exerce cette mission en plus de leurs fonctions dans l'établissement (de directeurs généraux de service pour plus du tiers d'entre eux). Une difficulté majeure est ainsi liée au manque de temps qu'ils peuvent consacrer aux missions de sécurité.

Les FSD sont en lien entre eux, avec le réseau des FSD de proximité et les services de l'Etat zonaux, notamment de renseignement (DGSI, DRSD, DNRT). La nature de ces relations dépend de l'organisation locale.

10. Confier aux FSD, dont l'autorité et l'expertise seraient réaffirmées, et en lien avec le déontologue, un rôle de formation et de sensibilisation de l'ensemble de la communauté académique sur les risques liés aux influences extra-européennes. Cette action serait renforcée dans les domaines ou les zones identifiées comme potentiellement les plus à risque par le document de référence.

ACTION MENÉE

La circulaire adressée aux chefs d'établissements le 25 mai 2023 précise que les FSD ont un rôle de diffusion d'une « culture de la sûreté et de la sécurité ». Les FSD, en lien avec les services spécialisés territorialement compétents, sont pleinement impliqués dans les actions de formation et de sensibilisation des usagers. Ces éléments

11. Élaborer et diffuser auprès des établissements via le réseau des FSD un guide de bonnes pratiques de coopération avec certains pays identifiés, guide qui doit être largement diffusé auprès de toute la communauté académique.

ACTION EN COURS

Un groupe de travail piloté par le SGDSN, dont la première réunion s'est tenue le 25 avril 2024 et auquel participent tous les ministères concernés par la réglementation relative à la PPST, travaille à fournir aux entités intéressées, notamment aux établissements d'ESR, un guide et une grille d'auto-évaluation préliminaire des projets de coopération.

Toutefois, il n'appartient pas au MESR, mais uniquement au SGDSN le cas échéant, de mettre à la disposition des établissements des documents relatifs à des Etats en particulier.

12. Assurer une sensibilisation des collectivités territoriales, notamment régions et les grandes métropoles sur ces sujets, compte tenu de leur place significative dans les conseils d'administration des établissements d'enseignement supérieur.

ACTION EN COURS

Le MESR est pleinement engagé dans la sensibilisation continue des acteurs aux problématiques d'influence, notamment à travers un plan de sensibilisation ministériel décidé en juillet 2022. Il prend forme via le réseau des délégations régionales académiques à la recherche et à l'innovation (DRARI) s'agissant de l'intelligence économique territoriale.

13. Étendre le bénéfice de la protection fonctionnelle à l'ensemble de la communauté académique (chercheurs non agents publics, institutions).

ACTION EN COURS

Le MESR, dans le cadre des travaux pilotés par le SGDSN sur l'instrumentalisation du droit à des fins stratégiques (« lawfare »), travaille à développer des solutions permettant de dépasser les limites actuelles de la protection fonctionnelle.

La direction des affaires juridiques pilote, depuis 2022, une enquête annuelle visant à identifier le nombre de procédures-bâillons intentées à l'encontre des personnels enseignants et chercheurs, ainsi que les suites données aux demandes de protection fonctionnelle en rapport direct avec ces procédures.

Dans les établissements d'enseignement supérieur, une dizaine de procédures-bâillons à l'encontre d'enseignants-chercheurs ou de chercheurs ont été recensées en 2022 (10) et en 2023 (8). Aucun cas n'a

permis d'identifier l'action, directe ou indirecte, d'un État étranger. 88 % des demandes ont abouti à l'octroi de la protection fonctionnelle.

Aucune procédure-bâillon n'a été relevée dans les établissements de recherche.

14. Généraliser la réalisation par l'autorité nationale en matière de sécurité et de défense des systèmes d'information (ANSSI) d'un audit sur la sécurité des systèmes informatiques des universités, en y intégrant la question de la confidentialité des cours en ligne.

ACTION NON ENGAGÉE

Les services du Premier ministre et leurs partenaires mettent à la disposition des établissements d'ESR un certain nombre de ressources et d'expertises portant sur la sécurité du numérique, systématiquement valorisées par le SDS.

Les établissements d'ESR, et notamment les universités, disposent d'une autonomie de gestion, qui empêchent toute généralisation prescriptive.

15. Renforcer les moyens dédiés à la détection et à la protection du monde universitaire et académique face aux interférences extérieures en inscrivant des crédits dédiés dans les budgets des universités et du ministère de l'Europe et des affaires étrangères.

ACTION EN COURS

Le MESR a exprimé un besoin de création, par des crédits dédiés, de 140 ETP en établissements d'ESR sur les missions des FSD. Cette action budgétaire est soumise à un arbitrage de haut niveau.

Objectif 3 : Ériger au niveau national la transparence et la réciprocité en principes cardinaux de toute coopération universitaire internationale

16. Prévoir, dans le cadre des décrets qui doivent être publiés au titre de l'article L. 211-2 du code de l'éducation, et en s'inspirant de l'article L. 411-5 du code de la recherche, l'obligation pour les chercheurs de signaler dans leurs thèses, travaux post doctoraux et publications scientifiques les éventuelles aides directes et indirectes dont ils ont pu bénéficier de la part d'États extra-européens.

ACTION EN PARTIE ENGAGÉE

L'instauration progressive d'un régime de transparence sur les financements et les liens d'intérêts extra-européens des chercheurs apparaît pertinente, au-delà des dispositions prévues à l'article L. 411-5 du code de la recherche qui ne concernent que les expertises réalisées auprès du Parlement ou des pouvoirs publics constitutionnels.

Dans le cadre de cette volonté de montée en puissance, un groupe de travail, piloté par le SGDSN, vise à permettre, de manière effective, d'exiger la déclaration par les candidats de leurs éventuels conflits d'intérêts dans les demandes d'accès aux zones à régime restrictif.

17. Créer un régime de transparence sur l'origine des financements extra-européens des projets (colloques, contrats doctoraux, chaires...) menés par les établissements d'enseignement supérieur et de recherche et les think-tanks.

ACTION NON ENGAGÉE

Les budgets des établissements publics – y compris d'ESR – sont publics et peuvent, le cas échéant, faire l'objet d'évaluations, d'inspections et de contrôles. Toutefois, le renforcement du régime de transparence sur les financements extra-européens dont bénéficient les établissements d'ESR apparaît pertinente.

18. Faire valoir au niveau national des exigences de réciprocité dans les échanges universitaires avec les pays extra européens.

ACTION MENÉE

À tous les niveaux et sur les plans stratégique, diplomatique, politique et technique, les services de l'État font valoir des exigences de réciprocité dans les échanges scientifiques et universitaires. Cet équilibre est une nécessité absolue dans la protection des intérêts fondamentaux de la Nation.

Les avis rendus par le SDS sur des projets d'accords de coopération sont fondés sur une analyse de risques coûts-avantages qui intègrent, face au risque de captation économique, une expertise technique sur les clauses de réciprocité.

Les actions de sensibilisation menés auprès des établissements et des FSD, le cas échéant en lien avec tous les services de l'État, promeuvent une grande vigilance sur ces sujets.

19. Inclure systématiquement une clause relative au respect des libertés académiques et de l'intégrité scientifique dans les conventions passées avec les institutions et entreprises extra-européennes.

ACTION NON ENGAGÉE

Les universités disposent d'une autonomie de gestion, qui ne permet pas de s'assurer de l'intégration systématique d'une clause relative au respect des libertés académiques et de l'intégrité scientifique dans les conventions passées entre les établissements et les institutions et entreprises extra-européennes.

Les avis rendus par le SDS veillent toutefois, avec diligence, à la bonne prise en compte de ces enjeux dans les projets d'accord impliquant un établissement français et un partenaire issu d'un pays sensible sur ces aspects.

Les actions de sensibilisation menés auprès des établissements et des FSD, le cas échéant en lien avec tous les services de l'État, promeuvent une vigilance sur ces sujets.

Objectif 4 : Renforcer les procédures administratives destinées à contrôler les partenariats passés par les établissements d'enseignement supérieur et de recherche

20. Modifier l'article L. 123-7-1 et l'article D. 123-19 du code de l'éducation pour prévoir une saisine pour avis des ministères concernés (enseignement supérieur et recherche, économie, affaires étrangères, intérieur et armées s'il y a lieu) sur les projets d'accord.

ACTION EN PARTIE ENGAGÉE

Dans les faits, la transmission des projets d'accords internationaux au titre de l'article L. 123-7-1 du code de l'éducation correspond à une saisine pour avis – notamment lorsque l'accord soumis relève des secteurs scientifiques et techniques protégés. L'avis rendu est non contraignant. L'article D. 123-19 du même code prévoit d'ores-et-déjà l'implication de toutes les administrations intéressées dans le processus d'examen.

Un groupe de travail piloté par le SGD&N, dont la première réunion s'est tenue le 25 avril 2024, et auquel participent tous les ministères concernés par la réglementation relative à la PPST, travaille à pouvoir instaurer, par voie réglementaire, une obligation de saisine pour avis sur les projets de coopération internationale en cas d'implication d'une unité de recherche protégée par le dispositif réglementaire. Le non-respect de cette obligation donnerait lieu à une contravention.

21. Modifier les mêmes articles pour fixer à trois mois maximum le délai d'examen des projets d'accord, pour permettre des investigations sérieuses.

ACTION NON ENGAGÉE

Le délai moyen d'expertise par le SDS des projets d'accords internationaux soumis par les établissements d'ESR est supérieur à trente jours. L'allongement du délai d'opposition prévu par l'article L. 123-7-1 du code de l'éducation, dont la modification relève du Parlement, apparaît pertinente.

Le SDS, en lien avec la délégation aux affaires européennes et internationales du MESR et le ministère de l'Europe et des affaires étrangères, développe toutefois un logiciel informatique qui devrait permettre un traitement plus efficace et unifiée des soumissions.

22. Prévoir que les accords de recherche passés avec les filiales françaises des entreprises étrangères extra-européennes soient soumis systématiquement à la procédure d'examen.

ACTION NON ENGAGÉE

Cette recommandation, qui relève du domaine législatif en ce qu'elle nécessite une modification de l'article L. 123-7-1 du code de l'éducation, apparaît pertinente dans son principe.

Une vigilance devrait, le cas échéant, être portée sur la définition des « filiales françaises des entreprises étrangères extra-européennes », notion généraliste, et sur les moyens d'expertise dédiés face à un accroissement conséquent du nombre de projets d'accord soumis pour examen. Cette mesure nécessite un important travail de coordination, en lien avec le SGDSN et les services du ministère chargé de l'économie.

Objectif 5 : Promouvoir au niveau national, européen et international l'adoption d'un référentiel de normes et de lignes directrices

23. Au niveau national, étudier l'adoption d'un corpus de moyens juridiques, d'ordre administratif et le cas échéant pénal, visant à sanctionner les interférences portant atteintes aux libertés académiques et à l'intégrité scientifique.

ACTION EN COURS

La loi protège la liberté académique, principe fondamental reconnu par les lois de la République, et l'intégrité scientifique respectivement aux articles L. 141-6, L. 123-9, L. 952-2 du code de l'éducation et à l'article L. 211-2 du code de la recherche. Il appartient aux établissements d'ESR de se conformer à leurs exigences. À cette fin, les établissements sont dotés d'un référent à l'intégrité scientifique (lettre-circulaire du 15 mars 2017) et d'un référent déontologique (loi du 20 avril 2016).

Les chercheurs et enseignants-chercheurs qui sont cibles d'atteintes à la liberté académique, notamment par des campagnes de dénigrement, sont dans la grande majorité des cas accompagnés par les services de l'État à travers la protection fonctionnelle (cf. recommandation n° 12).

Vis-à-vis de la PPST en particulier, le décret n° 2024-430 du 14 mai 2024 portant diverses dispositions relatives à la protection du potentiel scientifique et technique de la Nation prévoit une contravention de 5^e catégorie à l'égard de toute personne qui interfrérait dans la protection du potentiel scientifique et technique.

Le code pénal punit de manière générique, aux articles 411-2 à 411-11, les délits et crimes de trahison et d'espionnage – notamment lorsqu'ils prendraient la forme d'intelligences avec une puissance étrangère susceptibles de porter atteinte aux intérêts fondamentaux de la Nation.

24. Au niveau européen, mettre à profit la Présidence française de l'Union européenne pour proposer une stratégie ambitieuse de diplomatie scientifique, à la fois défensive, mais également offensive, dans la lignée du début de prise de conscience de nos partenaires.

ACTION MENÉE

La présidence française du Conseil de l'Union européenne (PFUE) a fait d'une meilleure structuration de la coopération internationale R&I l'une de ses priorités. La conférence ministérielle de Marseille du 8 mars 2022 a donné lieu à un débat des ministres sur la coordination de la coopération internationale R&I. Un atelier a été organisé sur la diplomatie scientifique pour avancer le débat européen sur le sujet, ce qui a contribué aux travaux en cours d'établir un cadre européen de diplomatie scientifique. La conférence a donné lieu à la déclaration de Marseille qui énonce neuf principes et valeurs pour une coopération internationale R&I équilibrée, dont la gestion des risques et la sécurité. Grâce à cette impulsion politique par la PFUE, la Commission européenne a lancé un dialogue multilatéral avec les principaux partenaires internationaux de la France pour promouvoir ces principes et valeurs.

25. Inciter au niveau européen et international à la création d'un classement des universités fondé sur le respect des libertés académiques et de l'intégrité scientifique, afin de mettre en lumière nos valeurs, par opposition à un classement de Shanghai devenu trop prescripteur.

À ce stade, le service ne formule pas d'observation sur cette recommandation.

26. Promouvoir une norme européenne et internationale de clarification des échanges universitaires fondée sur le devoir de diligence (due diligence) et la conformité (compliance) à des lignes directrices fondées sur le respect de la liberté académique et l'intégrité scientifique, en accord avec la déclaration de Bonn du 23 octobre 2020 et les travaux de l'OCDE.

ACTION MENÉE

Le dialogue multilatéral sur les valeurs et les principes de la coopération internationale en matière de R&I, lancée suite à l'impulsion de la PFUE promeut l'Union européenne comme une force normative dans ce domaine. Dans ce cadre ont été organisés des ateliers spécifiques sur les questions de liberté académique, d'intégrité académique et de la sécurité de la recherche. La France a été par ailleurs force motrice des travaux menés au Conseil de l'Union européenne, sous présidence belge, pour établir des recommandations s'adressant aux autorités nationales, mais aussi aux établissements d'enseignement supérieur, aux organismes de recherche et aux agences de financement. Les recommandations comprennent des principes directeurs pour une internationalisation responsable, des actions politiques clés au niveau national et sectoriel pour renforcer la sécurité de la recherche, ainsi que des actions au niveau de l'Union européenne pour soutenir les efforts des États membres et du secteur de la recherche. Lors des négociations, la France a défendu un texte très ambitieux.

S'agissant des activités menées dans le cadre de l'OCDE, la récente réunion ministérielle STI de fin avril 2024, présidée par la France ainsi que l'actuelle charte française de l'innovation responsable en neurotechnologies sont nodaux. Au sein du Comité de politiques scientifiques et technologies (CPST), la France soutient la conduite de travaux visant à une mise en œuvre de la déclaration et des documents, précités, auxquels celle-ci réfère. La France compte rester attentive à ce qu'un suivi régulier de cette mise en œuvre et des impacts afférents soit effectué au sein du CPST.

CONTRIBUTION DU GROUPE DE L'UNION CENTRISTE

La commission d'enquête sur les politiques publiques face aux opérations d'influences étrangères a réalisé ses travaux entre les mois de février et juillet 2024. Un rapport, fidèle aux auditions, a été présenté le 23 juillet 2024. Le groupe centriste considère toutefois opportun d'apporter sa contribution.

À titre liminaire, les membres du groupe de l'Union Centriste regrettent que les demandes faites au président, comme au rapporteur, de produire un plan d'orientation des travaux n'aient pu aboutir, créant une difficulté dans la lecture et la progression des auditions.

Une méthodologie plus thématique aurait peut-être permis d'évoquer plus de sujets. Les sénateurs de l'Union Centriste regrettent ce choix qui, de leur point de vue, affaiblit la pertinence du rapport.

La question de l'islam radical et des influences étrangères dans ce domaine a été peu traitée, mais le rapport a été opportunément complété par un amendement de président Dominique de Legge, reprenant des amendements présentés par Mesdames Goulet, Morin-Desailly et Monsieur Reichardt.

Les sénateurs du groupe centriste considèrent également que la question du rôle des Etats-Unis d'Amérique n'a pas été suffisamment traitée. Il en est notamment de l'impact des grandes entreprises américaine GAFAM et de l'extraterritorialité des lois américaines sur notre souveraineté et sur la protection de nos données. Les questions d'influences malveillantes en matière d'économie ont été évoquées mais elles auraient mérité une approche plus déterminée lorsque l'on sait les défis rencontrés en matière de souveraineté alimentaire ou de souveraineté du médicament dès lors que ces domaines stratégiques font également l'objet de guerres économiques.

Par ailleurs, les sénateurs centristes regrettent que la question des cabinets de conseil n'ait été évoquée que de façon incidente lors des auditions.

C'est pourquoi, sur le fond, le groupe de l'Union centriste, par la voix de ses membres au sein de la commission d'enquête, souhaite rappeler ses nombreuses contributions aux travaux évoqués dans le présent rapport. Il s'agit des travaux sur les questions liées au numérique et à la souveraineté numérique, ceux sur la radicalisation, le séparatisme et les principes de la République et ceux sur la suprématie du droit américain.

Ces travaux constants depuis près de neuf ans sont des marqueurs du groupe UC et méritent d'être rappelés car de nombreuses propositions concrètes et non incantatoires faites dans le cadre des travaux mentionnés restent en attente de mise en œuvre.

I. LES TRAVAUX SUR LE NUMÉRIQUE

Le rapport présenté doit faire état des travaux antérieurs du Sénat sur les questions de gouvernance, de régulation et de politique relative au numérique. Les nombreux travaux effectués depuis 2013 visaient d'emblée à alerter de la manière dont l'Internet, le réseau des réseaux, était en train de se constituer, avec toutes les perspectives de développement, de progrès, mais aussi tous les dysfonctionnements déjà à l'œuvre qui n'ont fait que se renforcer.

1. « **L'Union européenne, colonie du monde numérique ?** » de Catherine MORIN-DESAILLY, déposé le 20 mars 2013
(<https://www.senat.fr/rap/r12-443/r12-443.html>)

Premier rapport « fondateur » pour le Sénat qui est bien cité dans le rapport de notre collègue Rachid Temal, mais avec une erreur sur la date : ce n'est pas 2023 mais 2013 [*erreur matérielle rectifiée*].

2. « **L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne** » de Catherine MORIN-DESAILLY
(<https://www.senat.fr/rap/r13-696-1/r13-696-117.html>)

Ce rapport du 8 juillet 2014, est issu de la mission commune d'information « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance de l'Internet » demandée par le groupe UC, à laquelle avaient alors participé tous les groupes politiques et toutes les commissions du Sénat.

10 ans de constats alarmistes et peu d'avancées

Cette mission avait été proposée au lendemain de l'affaire Snowden qui révéla au monde la surveillance et l'ingérence des Etats-Unis via les portes dérobées des plateformes. C'est le premier rapport du Sénat sur des ingérences étrangères, et le début d'une prise de conscience de la manipulation de l'information, de la surveillance en ligne. Il établit dans ses conclusions que l'Internet marque le nouveau tournant de l'affrontement mondial pour la domination du monde par l'économie et la connaissance.

Suite à ce constat, le rapport établissait 50 propositions, dont certaines suivies d'effets comme la mise en place du RGPD, la réforme de la direction du renseignement ou la réouverture de la directive e-commerce pour constituer le DMA et le DSA, avec encore des insuffisances mentionnées dans des rapports (Rapport d'information sur « Proposition de résolution au nom de la commission des affaires européennes, en application de l'article 73 quater du Règlement, sur la proposition de règlement sur les marchés numériques (DMA) : Proposition de règlement sur les marchés numériques (DMA) » du 7 octobre 2021 : <https://www.senat.fr/rap/r21-034/r21-034.html>) réalisés par Catherine Morin-Desailly et Florence Blatrix Contat (PS) au nom de la Commission des Affaires Européennes ou des propositions de résolution européenne votées à l'unanimité du Sénat.

3. « Proposition de résolution présentée en application de l'article 73 quinzièmes du Règlement, pour une stratégie européenne du numérique globale, offensive et ambitieuse » (<https://www.senat.fr/leg/ppr14-423.html>) de Catherine MORIN-DESAILLY

Cette proposition de résolution du 4 juin 2015, s'inscrit dans la continuité des travaux menés au Sénat sur le numérique, en particulier suite aux deux rapports précédemment cités et celui du 8 juillet 2014 « L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne ». (<https://www.senat.fr/rap/r13-696-1/r13-696-11.pdf>)

Plusieurs autres propositions du rapport de 2015 restent à réaliser : propositions permettant de construire une vraie souveraineté, une meilleure protection, une régulation du réseau des réseaux face aux ingérences, la formation de tous (proposition complétée dans un rapport fait au nom de la commission de la culture « Prendre en main notre destin numérique : l'urgence de la formation » (<https://www.senat.fr/rap/r17-607/r17-607.html>) du 27 juin 2018, qui proposait l'éducation aux médias et aux réseaux sociaux.

Le rapport préconise aussi de revoir la gouvernance mondiale du numérique.

4. Lutte contre les fausses informations (2018) de Catherine MORIN-DESAILLY
(<https://www.senat.fr/dossier-legislatif/ppl17-623.html>)

Le rapport vise à un meilleur contrôle des diffusions d'information par les plateformes, les obligeant pour certaines à fournir des données agrégées sur les contenus proposés aux internautes, les incitant à la conclusion d'accords de coopération relatifs à la lutte contre la diffusion de fausses informations, et préconisant la formation au numérique.

Plus généralement, il s'agit d'instaurer une obligation pour les plateformes d'assurer une visibilité améliorée des informations d'intérêt public émanant de sources fiables, notamment de sources journalistiques et de médias, sur la base de normes et de critères co-construits avec les acteurs du secteur. Plus concrètement, il s'agit de faciliter les notifications, pour pouvoir engager plus facilement la responsabilité des hébergeurs :

- en créant un « bouton » d'accès à l'interface de notification des contenus présumés illicites commun à tous les hébergeurs ;
- en élargissant la définition des « signaleurs de confiance », afin que ce statut puisse être accordé à certaines entités représentant des intérêts particuliers, telles que des marques, des sociétés de gestion de droits d'auteur, ou des journalistes, dans le cadre d'activités de vérification de faits ;
- en exigeant des fournisseurs de services en ligne des données chiffrées sur les moyens technologiques, financiers et humains qu'elles allouent à la modération, ventilés par pays et par langue.

5. Le numérique « grande cause nationale »

Le rapporteur propose que l'année 2025 devienne grande cause nationale pour l'éducation aux médias. En effet se prémunir des fausses nouvelles, de toute forme de manipulation sur internet et les réseaux nécessite d'armer plus largement les élèves et leurs enseignants.

En 2020, Catherine Morin-Desailly avait fait une demande similaire au Président de la République en 2020 « Pour une montée en compétence numérique pour tous », rappelant l'importance de l'éducation aux médias et aux réseaux sociaux, à la compréhension de notre écosystème et la formation des formateurs. Demande restée sans réponse.

6. Statut des plateformes : Responsabilisation partielle des hébergeurs (<https://www.senat.fr/leg/ppr17-739.html>)

Cette proposition de résolution du 27 septembre 2018 de Catherine Morin-Desailly demandait une évolution du cadre légal pour créer un statut intermédiaire entre celui d'hébergeur et celui d'éditeur, devant être compatible avec, d'une part, la liberté d'expression, d'autre part, avec le développement du marché intérieur et la croissance économique équilibrée.

II. LES TRAVAUX SUR LA SOUVERAINETE DU DROIT AMERICAIN

Le groupe Union Centriste souhaite rappeler les travaux importants menés par le sénateur Philippe Bonnecarrère : l'importance des GAFAM, les enjeux de la protection des données... constituent autant de sujets sur lesquels le groupe de l'Union Centriste a montré son investissement. (Proposition de résolution du 4 octobre 2018 au nom de la commission des affaires européennes sur l'extraterritorialité des sanctions américaines : Extradition des sanctions américaines : Quelles réponses de l'Union européenne ?

(https://www.senat.fr/rap/r18-017/r18-017_mono.html)

III. LES TRAVAUX SUR L'ISLAM, LE DJIHADISME, LE TERRORISME ET LE SEPARATISME

1. Filières « djihadistes » : pour une réponse globale et sans faiblesse (2015) (<https://www.senat.fr/rap/r14-388/r14-388.html>)

Le groupe de l'Union Centriste a été précurseur dans ce domaine ayant été à l'origine de la première commission d'enquête sur l'organisation et les moyens de la lutte contre les réseaux djihadistes en France et en Europe dont est issu ce rapport du 1^{er} avril 2015.

2. Organisation, place et financement de l'Islam

a. Financement des lieux de culte

Le sénateur Hervé Maurey a contribué aux travaux parlementaires sur le financement des lieux de culte avec un rapport d'information « Les collectivités territoriales et le financement des lieux de culte » (<https://www.senat.fr/rap/r14-345/r14-3451.pdf>) déposé au Sénat le 17 mars 2015.

Une des propositions phare ne figure toujours pas dans notre arsenal juridique consistant, lors du dépôt d'un permis de construire d'un lieu de culte, à joindre un plan de financement. Cette question réglerait la question de transparence du financement de tous les lieux de culte.

b. Proposition de résolution suivie du rapport de mission

La proposition de résolution du 27 novembre 2015 visait à la création d'une commission d'enquête sur l'organisation, la place et le financement de l'Islam en France et de ses lieux de culte (<https://www.senat.fr/leg/ppr15-203.html>).

La mission d'information « sur l'organisation, la place et le financement de l'Islam en France et de ses lieux de culte », constituée à l'initiative du groupe de l'UDI-UC dans le cadre de son « droit de tirage » a donné lieu à un rapport déposé le 5 juillet 2016 « De l'Islam en France à un Islam de France, établir la transparence et lever les ambiguïtés » (<https://www.senat.fr/rap/r15-757/r15-757.html>)

3. Radicalisation

Nathalie Goulet a déposé une proposition de loi le 7 octobre 2019 sur la prévention et la lutte contre la radicalisation. Elle a apporté sa contribution dans le tome I du rapport déposé le 7 juillet 2020 intitulé « Radicalisation islamiste : faire face et lutter ensemble » (https://www.senat.fr/rap/r19-595-1/r19-595-1_mono.html#toc722).

IV. AUTRES PROPOSITIONS DU GROUPE UNION CENTRISTE

Les sénateurs UC souhaitent ajouter deux recommandations qui n'ont pas pu être intégrées au rapport et qui pourtant sont en ligne directe avec le sujet :

- La création d'une délégation au numérique dans les deux assemblées ;
- Le rôle des cabinets de conseil évoqués incidemment lors des auditions.

1. Délégation parlementaire au numérique

(<https://www.senat.fr/dossier-legislatif/ppl23-712.html>)

Le 27 juin 2024, une proposition de loi visant à la création d'une délégation parlementaire au numérique a été déposée au Sénat. Une telle délégation permettrait tout à la fois au Parlement d'embrasser l'entièreté de la problématique numérique de manière transversale (son utilisation, la souveraineté, y compris les cryptoactifs) et de pouvoir travailler de façon continue avec le recul qui s'impose.

2. Influence croissante des cabinets de conseil sur les politiques publiques

Le groupe de l'UC regrette que la commission d'enquête n'ait pas étendue ses travaux au rôle des cabinets de conseil suivant les travaux menés par Éliane Assassi et Arnaud Bazin (<https://www.senat.fr/notice-rapport/2021/r21-578-1-notice.html>). Il a été établi que ces cabinets de conseil pouvaient constituer des vecteurs d'influences étrangères.

DOCUMENT PROVISOIRE

LISTE DES PERSONNES ENTENDUES

I. AUDITIONS EN RÉUNION PLÉNIÈRE

Mardi 27 février 2024 :

- Capitaine de vaisseau Yann **BRIAND**, sous-directeur des affaires internationales du secrétariat général de la défense et de la sécurité nationale (SGDSN)

Jeudi 29 février 2024 :

- MM. David **COLON**, enseignant-chercheur à Sciences-Po Paris, Nicolas **TENZER**, président du Centre d'étude et de réflexion pour l'action politique (Cerap) et Frédéric **CHARILLON**, professeur en science politique et relations internationales

Jeudi 7 mars 2024 :

- Mme Maud **QUESSARD**, directeur de recherche à l'Institut de recherche stratégique de l'école militaire (Irsem), MM. Maxime **AUDINET**, chercheur à l'Irsem, et Laurent **CORDONIER**, directeur de la recherche à la fondation Descartes

Mardi 12 mars 2024 :

- M. Christophe **LEMOINE**, directeur adjoint à la direction de la communication et de la presse du ministère de l'Europe et des affaires étrangères

Mardi 19 mars 2024 :

- Mme Elsa **PILICHOWSKI**, directrice de la gouvernance publique de l'Organisation de coopération et de développement économiques (OCDE)
- M. Roch-Olivier **MAISTRE**, président de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom)

Jeudi 21 mars 2024 :

- Mme Céline **BERTHON**, directrice générale de la sécurité intérieure
- Mme Teija **TIILIKAINEN**, directrice du centre d'excellence d'Helsinki en matière de lutte contre les menaces hybrides

Jeudi 28 mars 2024 :

- M. Jean-Philippe **VACHIA**, président de la Commission nationale des comptes de campagne et des financements politiques (CNCCFP)
- M. Henri **VERDIER**, ambassadeur pour le numérique

Jeudi 4 avril 2024 :

- Général de division Aymeric **BONNEMAISON**, commandant de la cyberdéfense de l'état-major des armées
- M. Etienne **APAIRE**, secrétaire général du comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR)

Mardi 9 avril 2024 :

- M. Joffrey **CÉLESTIN-URBAIN**, chef du service de l'information stratégique et de la sécurité économique (Sisse)
- MM. Thomas **HUCHON**, journaliste réalisateur spécialiste de la lutte contre la désinformation et les réseaux sociaux, et Gérald **HOLUBOWICZ**, journaliste expert en IA générative, sur l'intelligence artificielle et les manipulations de l'information

Mardi 30 avril 2024 :

- Mme Anne-Sophie **AVÉ**, ambassadrice pour la diplomatie publique en Afrique
- Mme Florence **PHILBERT**, directrice générale des médias et des industries culturelles

Jeudi 2 mai 2024 :

- Général de brigade Pascal **IANNI**, directeur du pôle « anticipation, stratégie et orientations » de l'état-major des armées
- MM. Edouard **GEFFRAY**, directeur général de l'enseignement supérieur, et Benjamin **LEPERCHEY**, chef de service, adjoint à la direction générale de l'enseignement scolaire et de l'insertion professionnelle

Mardi 14 mai 2024 :

- M. Thierry **LE GOFF**, secrétaire général, et Christophe **PEYREL**, chef du service de défense et de sécurité du ministère de l'éducation nationale et de la jeunesse

- MM. Grégoire **LEMARCHAND**, rédacteur en chef Investigation numérique à l'Agence France Presse (AFP), Vincent **COURONNE**, directeur général de « Les Surligneurs » et Mme Anaïs **CONDOMINES**, rédactrice en chef adjointe de la rubrique CheckNews de Libération

Jeudi 16 mai 2024 :

- M. Jean-Marie **BOCKEL**, envoyé personnel du Président de la République pour l'Afrique
- M. Bernard **ROUGIER**, professeur des universités (*audition rapporteur*)

Jeudi 23 mai 2024 :

- M. Didier **MIGAUD**, président de la Haute autorité pour la transparence de la vie publique (HATVP)
- Mmes Béatrice **OEUVRARD** et Elisa **BORRY-ESTRADE**, responsables des affaires publiques de Meta France

Mardi 28 mai 2024 :

- M. Nicolas **LERNER**, directeur général de la sécurité extérieure
- MM. Frédéric **GÉRAUD DE LESCAZES**, directeur des relations institutionnelles de Google Cloud France, David **GROUT**, directeur technique de « Mandiant » et Thibault **GUIROY**, directeur des relations institutionnelles de YouTube France
- M. Gérald **DARMANIN**, ministre de l'intérieur et des Outre-Mer

Mercredi 29 mai 2024 :

- M. Jean-Noël **BARROT**, ministre délégué chargé de l'Europe

Jeudi 30 mai 2024 :

- M. Antoine **MAGNANT**, directeur général de Tracfin
- Mme Claire **DILÉ**, directrice des affaires publiques de X France

Mardi 4 juin 2024 :

- M. Éric **GARANDEAU**, directeur des affaires publiques de TikTok France

- MM. Tariq **KRIM**, fondateur du think tank Cybernetica, Bernard **BENHAMOU**, secrétaire général de l’Institut de la souveraineté numérique, Julien **NOCETTI**, chercheur au Centre d’analyse, de prévision et de stratégie du ministère des affaires étrangères, David **CHAVALARIA**, directeur de recherche au CNRS

Jeudi 6 juin 2024 :

- M. Paul **CHARON**, directeur du domaine « renseignement, anticipation et stratégies d’influence » à l’Institut de recherche stratégique de l’École militaire (Irsem)
- Mme Marie-Christine **SARAGOSSE**, présidente-directrice générale de France Médias Monde

Mardi 11 juin 2024 :

- M. Stéphane **BOUILLO**N, secrétaire général de la défense et de la sécurité nationale
- M. Claude **MALHURET**, rapporteur de la commission d’enquête sur l’utilisation du réseau social tiktok, son exploitation des données, sa stratégie d’influence (*audition rapporteur*)

Jeudi 13 juin 2024 :

- MM. Antoine **BERNARD**, directeur « Plaidoyer et Assistance » et Thibaut **BRUTTIN**, adjoint au directeur général, Reporters sans frontières

Mardi 18 juin 2024 :

- Mme Sylvie **RETAILLEAU**, ministre de l’enseignement supérieur et de la recherche
- M. Stéphane **SÉJOURNÉ**, ministre de l’Europe et des affaires étrangères
- M. Aurélien **LECHEVALLIER**, directeur général de la mondialisation, de la culture, de l’enseignement et du développement international au ministère de l’Europe et des affaires étrangères (*audition rapporteur*)

Jeudi 20 juin 2024 :

- M. Guy-Philippe **GOLDSTEIN**, consultant sur les questions de cyber-sécurité

Mardi 25 juin 2024 :

- M. Sébastien LECORNU, ministre des armées

II. AUDITIONS DU RAPPORTEUR

Lundi 6 mai 2024 :

- M. André GATTOLIN, sénateur

Lundi 13 mai 2024 :

- Mmes Sacha HOULIÉ et Constance LE GRIP, députés

Jeudi 16 mai 2024 :

- M. Bernard ROUGIER, professeur des universités

Lundi 3 juin 2024 :

- MM. Guillaume GELLÉ, président de France Universités et Jean-François HUCHET, président de l'Institut national des langues et civilisations orientales (Inalco)

- M. Patrice BRODEUR, professeur agrégé à l'Institut d'études religieuses à la Faculté des arts et des sciences de l'Université de Montréal

Lundi 17 juin 2024 :

- M. Marc-Antoine BRILLANT, chef du service de vigilance et de protection contre les ingérences numériques étrangères, et Mme Anne-Sophie DHIVERT, cheffe adjointe du service, M. Hervé LETOQUEUX, chef de la division des opérations, Mmes Claire BENOÎT, cheffe du bureau coordination et stratégie

Lundi 24 juin 2024 :

- M. Olivier ROY, politologue et universitaire, spécialiste de l'Islam
- Mme Cécile CALÉ, co-fondatrice de MuseIA
- Mme Laureline PEYREFITTE, directrice des affaires criminelles et des grâces au ministère de la justice
- MM. François GOUYETTE, ancien ambassadeur de France et Pascal COURTADE, préfet

Mardi 25 juin 2024 :

- Mme Olivia **PENICHOU**, déléguée à l'information et à la communication de la défense

DOCUMENT PROVISOIRE

LISTE DES DÉPLACEMENTS

Visite du service de vigilance et protection contre les ingérences numériques étrangères (Viginum), 5 mars 2024 :

- Visite des locaux et entretien avec **MM. Marc-Antoine Brillant**, chef du service de vigilance et de protection contre les ingérences numériques étrangères, **Hervé Letoqueux**, chef de la division des opérations, et **Mme Laura Brincourt**, pôle coordination et stratégie.

Déplacement à Bruxelles, 11 avril 2024 :

Représentation permanente de la France auprès de l'Union européenne :

- Entretien avec **M. Philippe LEGLISE-COSTA**, Représentant permanent

Commission européenne :

- Entretien avec **Mme Eleonara OCELLO**, conseillère de M. Thierry BRETON, commissaire européen au marché intérieur

Parlement européen :

- Entretien avec **Mme Nathalie LOISEAU**, députée européenne (France - Renew) et **M. Arnaud DANJEAN**, député européen (France - PPE)

OTAN :

- Entretien avec **Mme Muriel DOMENACH**, Représentante permanente de la France auprès de l'Otan
- Entretien avec **Mme Marie-Doha BESANCENOT**, directrice adjointe des relations publiques de l'Otan

Service européen pour l'action extérieure :

- Entretien avec **Mme Aude MAIO-COLICHE**, directrice Communication stratégique et prospective

Déplacement à Taïwan du rapporteur¹, 22 mai 2024 :

Entretien avec M. Yen-Num Huang, Ministre des affaires numériques de Taïwan.

Déplacement à Rennes, 10 juin 2024 ::

- Visite du groupement de la cyberdéfense des armées (GCA) du Commandement de la cyberdéfense (Comcyber) et entretien avec le Colonel Nicolas Pierson, commandant du GCA, le Capitaine de vaisseau Olivier de France, chef du pôle opérations du Comcyber, le lieutenant-colonel Benoît Schnoebelen, chef du groupement des opérations numériques et N., officier du centre interarmées des actions sur l'environnement (CIAE) ;
- Entretien avec MM. Loic Roignant, délégué général du Pôle d'excellence Cyber (PEC) et Jean Luc Gibernon (SopraSteria), vice-président, et table ronde avec les membres du groupe de travail sur la lutte contre les manipulations de l'information : , : M. Jean Philippe Riant, directeur conseil en intelligence artificielle et communication digitale, Mme Brunessen Bertrand, professeur à l'université de Rennes, spécialisée sur le sujet des LMI, Mme Aurélie Laize (Airbus), MM. Jean-Mathieu Tilquin (Sahar) et Alban Ondrejeck (AnozrWay)
- Visite du site de Bruz de la direction générale de l'armement - maîtrise de l'information (DGA-MI)

Déplacement en Finlande et en Estonie, du 26 au 28 juin 2024 :

Helsinki, Finlande

Ambassade de France en Finlande :

- Entretien avec **Mme Agnès Cukierman**, Ambassadrice, **Mme Claire Durand**, attachée de défense, **MM. Christophe Manesse**, premier secrétaire, **Joël Ferrand**, attaché de presse et **Thibaut de Maistre**, stagiaire INSPet

Centre d'excellence pour la lutte contre les menaces hybrides :

- Entretien avec **Mme Teija Tiilikainen**, directrice et **M. Maxime Lebrun**, directeur adjoint recherches et analyse

¹ Entretien effectué dans le cadre du déplacement d'une délégation parlementaire conduite par M. Rachid Temal, composée de Mmes Else Joseph, sénatrice, Marie-Noëlle Battistel, députée, M. Hadrien Ghomi, député, à l'occasion de l'investiture le 20 mai 2024 de M. Lai Ching-te, président de Taïwan.

Parlement de Finlande :

- Entretien avec MM. **Jukka Kopra**, président de la commission de la défense, **Mats Löström**, député des îles Åland, membre de la commission des transports et des communications, et M. **Mika Boedeker**, secrétaire de la commission des transports et communications

Agence nationale des approvisionnements d'urgence (NESI) :

- *Entretien avec M. Janne Käkkänen*, directeur, Mme **Johanna Räty**, spécialiste des relations internationales

Institut National de l'audiovisuel (KAVI) :

- Entretien avec **Mme Saara Salomaa**, cheffe du service pour l'éducation aux médias et les médias audiovisuels

Faktabaari :

- Entretien avec **M. Kari Kivinen**, directeur d'école, fondateur de Faktabaari, Mme **Elsa Kivinen**, contributrice, et M. Guillaume Kuster, président et co-fondateur de Check First

Tallinn, Estonie

Ambassade de France en Estonie :

- *Entretien avec M. Emmanuel Mignot*, Ambassadeur, en présence de MM. **Florent Cheval**, premier conseiller, **Frédéric Contal**, attaché de défense, **Alexandre Sastre**, conseiller politique, et **Ulysse Guérin**, stagiaire INSP
- Entretien avec le **Lieutenant-Colonel Uku Arold**, chef de la communication stratégique des forces de défense estoniennes, et M. **Roland Murof**, chef adjoint du département de la communication stratégique du ministère de la défense estonien

Parlement d'Estonie :

- Entretien avec MM. **Leo Kunnas**, Vice-Président de la Commission de la défense, et **Aivar Engel**, administrateur

Propastop :

- *Entretien avec M. Andres Lember*, fondateur de Propastop, association de lutte contre les menaces informationnelles

Centre d'excellence de cyberdéfense coopérative de l'OTAN (CCDCOE) :

- *Entretien avec le Commandant **Jack Shis**, directeur adjoint et **Mme Angelica Tikk**, directrice des relations internationales*

Chancellerie d'État :

- *Entretien avec **MM. Rain Puusta**, conseiller en communication stratégique, **Priit Talv** et **Mme Stella Saarts**, spécialistes en lutte contre les ingérences informationnelles*

Ministère des affaires étrangères :

- Entretien avec **M. Mihkel Tamm**, directeur général de la communication

International Center for Defence and Security :

- *Entretien avec **M. Marek Kohv**, chercheur et directeur du Programme Sécurité et Résilience*

Visite de l'Agence nationale de la sécurité des systèmes d'information (Anssi) à Paris, 2 juillet 2024 :

- Entretiens avec **M. Vincent Strubel**, directeur général, **Mme Jennyfer Chrétien**, directrice de cabinet, **MM. Mathieu Feuillet**, sous-directeur Opérations et **Renaud Labelle**, sous-directeur Expertise
- Visite de la permanence opérationnelle et du laboratoire d'expertise

TABLEAU DE MISE EN ŒUVRE ET DE SUIVI

N°	Recommandation	Acteurs concernés	Calendrier prévisionnel	Support
La nécessité de refonder notre approche collective du phénomène				
1	Engager sans délai des recherches académiques transdisciplinaires sur la perception et la réception des opérations de manipulation de l'information sur l'individu et la société, et veiller à l'actualisation régulière de nos connaissances en la matière	Ministère de l'enseignement supérieur et de la recherche, Agence nationale de la recherche, établissements d'enseignement supérieur et de recherche	Immédiat	Appels à projets de l'Agence nationale de la recherche (notamment)
2	Élaborer une stratégie globale, nationale et interministérielle de lutte contre les influences étrangères malveillantes, en intégrant d'emblée les enjeux de financement et en associant le Parlement. Un débat sur sa mise œuvre se tiendrait annuellement au sein des assemblées	SGDSN	Immédiat	Document public
3	Établir une doctrine claire en matière de réponse aux opérations d'influence malveillantes	SGDSN, Ministère de l'Europe et des affaires étrangères, Ministère des armées	Immédiat	Document interne confidentiel
4	Conforter Viginum dans son rôle de chef-de-file en matière de protection du débat public numérique, en lui conférant un statut d'agence de l'État dotée d'une autonomie de gestion et placée sous la tutelle du secrétariat général de la défense et de la sécurité nationale (SGDSN)	Premier ministre, SGDSN	2025	Décret

5	Réaffirmer le portage politique par le Premier ministre de la politique de lutte contre les influences étrangères malveillantes en la confortant par la désignation d'un membre du Gouvernement placé auprès de lui qui en aurait la charge	Président de la République, Premier ministre	Immédiat	Décision du Président de la République sur proposition du Premier ministre
6	Mettre en place un observatoire des influences étrangères malveillantes regroupant les parties prenantes de la société civile et les acteurs publics concernés	SGDSN, Ministère de l'enseignement supérieur et de la recherche, Ministère de la culture (notamment)	Immédiat	Décision du Gouvernement
Lutter contre les influences étrangères malveillantes sur le territoire national				
7	Conférer à Viginum des moyens humains et matériels en adéquation avec sa mission de chef de file en matière de protection du débat public numérique et identifier clairement, au sein des documents budgétaires et dans une logique de transparence, les crédits et les effectifs alloués	SGDSN, Viginum, Ministère de l'économie et des finances, Parlement	Immédiat	Loi de finances
8	Renforcer les moyens juridiques de Viginum, en : supprimant la référence au seuil des 5 millions de visiteurs uniques par mois pour les plateformes en ligne ; autorisant la collecte automatisée de données dans les activités de veille de Viginum ; allongeant le délai de conservation des données traitées et le délai de renouvellement des collectes ; revoyant la notion d'ingérence numérique étrangère	SGDSN, Viginum	2024	Modification du décret n° 2021-922 du 13 juillet 2021 et du décret n° 2021-1587 du 7 décembre 2021

9	<p>Se doter d'un outil de suivi des investissements étrangers en France à l'aune non plus seulement, comme le fait le service de l'information stratégique et de la sécurité économique (Sisse), du caractère stratégique de leur objet mais de leur possible finalité d'influence à moyen-long terme</p>	Sisse	2025	Décret
10	<p>Mettre pleinement en œuvre le volet pénal de la loi « Ingérences étrangères », en diffusant largement aux magistrats l'information pertinente sur les nouveaux outils de lutte contre les ingérences étrangères et en intégrant pleinement la caractérisation de la nouvelle circonstance aggravante d'ingérence étrangère dans la coopération entre Pharos et Viginum. Intégrer cette dimension dans la formation des magistrats à l'École nationale de la magistrature</p>	Ministère de la justice	Immédiat	Circulaires pour les parquets et les juridictions, mise à jour des « Focus DACG »
<p>Dans le champ des armées, réévaluer les moyens budgétaires à l'aune des nouvelles menaces</p>				
11	<p>Réévaluer, à l'occasion de la prochaine actualisation de la loi de programmation militaire, soit avant la fin de l'année 2027, les moyens de la lutte informationnelle à l'aune de l'évolution de la menace</p>	Ministère des armées	2027	<p>Actualisation de la loi n° 2023-703 du 1^{er} août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense</p>

Développer notre influence positive à l'étranger en l'articulant à la politique de lutte contre les influences malveillantes				
12	Renforcer les dispositifs de veille et d'alerte au sein du ministère de l'Europe et des affaires étrangères, notamment en : développant les capacités de veille et d'enquête en sources ouvertes au sein de la sous-direction « veille et stratégie » de la direction de la presse et de la communication ; poursuivant les efforts de formation du réseau diplomatique aux enjeux de communication stratégique	Ministère de l'Europe et des affaires étrangères	Immédiat	Loi de finances
13	Renforcer, dans le cadre du prochain contrat d'objectifs et de moyens, les capacités de France Médias Monde pour lutter contre la désinformation	Ministère de l'économie et des finances, ministère de l'Europe et des affaires étrangères, ministère de la culture, ministère chargé des comptes publics, France Médias Monde	2024	Contrat d'objectifs et de moyens entre l'État et France Médias Monde 2024-2026
14	Rendre plus accessible les offres de radio de France Médias Monde en langue étrangère sur le territoire français grâce à la radio numérique terrestre (DAB +)	France Médias Monde, Radio France Internationale	Immédiat	Autorisation de l'Arcom
15	Étendre la diffusion de France 24, notamment en Chine	Ministère de l'Europe et des affaires étrangères, France Médias Monde, France 24	Immédiat	Relations diplomatiques bilatérales
16	Poursuivre les efforts visant à faire d'Arte une « plateforme européenne de référence »	Ministère de la culture	Immédiat	Décision du Gouvernement
17	Créer une « Pléiade d'influence » d'écrivains, scénaristes et	Ministère de l'Europe et des affaires	Immédiat	Décision du Gouvernement

	représentants des différentes disciplines artistiques au service de la politique d'influence et de la diplomatie publique	étrangères, ministère de la culture		
Renforcer les capacités communes de détection et de riposte de la France et de ses alliés				
18	Amplifier l'engagement de la France pour porter l'enjeu de la lutte contre les « FIMI » au niveau de l'Union européenne, de l'Otan, de l'OCDE et du G7, et renforcer les capacités de riposte collectives	Ministère de l'Europe et des affaires étrangères	Immédiat	Négociations diplomatiques multilatérales
19	Accompagner les partenaires européens souhaitant se doter de capacités comparables à Viginum	Viginum	Immédiat	Coopération bilatérale interservices
20	Accompagner les partenaires de l'Otan souhaitant se doter de capacités comparables à celles du Comcyber	Comcyber	Immédiat	Coopération bilatérale interservices
21	Compléter le mandat de l'Arcom pour y intégrer la thématique de la prévention des ingérences étrangères	Ministère de la culture, Parlement	Immédiat	Modification de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication
22	Rétablissement une obligation de conventionnement avec l'Arcom pour les médias audiovisuels extra-européens	Ministère de la culture, Parlement	Immédiat	Modification de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication
23	À l'occasion d'une prochaine révision de la directive « SMA », proposer une simplification de l'application des critères utilisés pour déterminer l'État membre compétent au titre d'un média audiovisuel extra-européen	Ministère de l'Europe et des affaires étrangères	Immédiat	Négociations au niveau de l'Union européenne

24	<p>Sur le modèle du dispositif prévu à l'article L. 163-2 du code électoral, mettre en place un dispositif permettant à l'autorité judiciaire de faire cesser la diffusion massive et artificielle de contenus faux ou trompeurs rattachables à une ingérence numérique étrangère et de nature à porter atteinte aux intérêts fondamentaux de la Nation</p>	<p>Ministère de la culture, Ministère de la justice, Parlement</p>	Immédiat	Loi
25	<p>À court terme, exploiter pleinement les nouvelles prérogatives de régulation conférées par le règlement de l'Union européenne sur les services numériques (DSA) pour s'assurer que les plateformes se donnent les moyens de lutter contre les manipulations de l'information liées à des opérations d'ingérences informationnelles</p>	<p>Arcom</p>	Immédiat	Action de l'Arcom
26	<p>À moyen terme, porter au niveau européen une position tendant à conférer aux plateformes un statut d'éditeur au titre d'une partie des contenus qu'ils diffusent ou, à minima, leur conférer un statut hybride d'« entités structurantes de l'espace informationnel » (ni-hébergeur, ni éditeur) assorti d'obligations spécifiques permettant de prévenir les ingérences informationnelles</p>	<p>Ministère de l'Europe et des affaires étrangères</p>	À engager immédiatement	Négociations au niveau de l'Union européenne

27	Se donner les moyens d'une politique industrielle volontariste en faveur de la souveraineté numérique française et européenne, avec pour objectif de long terme que notre espace informationnel cesse d'être structuré par des opérateurs extra-européens	Ministère de l'économie et des finances, Ministère de l'Europe et des affaires étrangères	À engager immédiatement	Politique industrielle du Gouvernement, négociations au niveau de l'Union européenne
28	Identifier spécifiquement les menaces liées aux ingérences étrangères dans les contrats d'objectifs et de moyens passés entre l'État et les médias réalisant des missions d'intérêt général, en prévoyant notamment la mise en place de dispositifs internes de protection sur le modèle de la procédure d'alerte mise en place par France Médias Monde	Ministère de la culture (DGMIC)	2024	Contrat d'objectifs et de moyens entre l'État et les entreprises audiovisuelles publiques 2024-2026
Renforcer les instruments de contrôle de la vie publique et politique à l'aune du risque d'ingérence				
29	Combler les lacunes existantes dans le cadre juridique applicable au financement des campagnes électorales et des partis politiques, en limitant le montant des prêts à un candidat ou à un parti politique, en interdisant aux personnes physiques étrangères ne résidant pas en France de consentir à ce type de prêts, et en interdisant aux mêmes personnes de cotiser aux partis politiques	Ministère de l'intérieur et des Outre-mer, Parlement	Immédiat	Modification du code électoral (partie législative)
30	Interdire aux partis et aux candidats de recourir aux créateurs de contenus sur les plateformes (« influenceurs ») pour mener des campagnes d'influence électorale rémunérées	Ministère de l'intérieur et des Outre-mer, Parlement	Immédiat	Modification du code électoral (partie législative)

31	<p>Renforcer les prérogatives de la Commission nationale des comptes de campagnes et des financements politiques (CNCCFP), en lui permettant de demander aux prêteurs d'établir l'origine des fonds prêtés à un candidat ou à un parti politique, d'accéder au fichier national des comptes bancaires (Ficoba) et en l'intégrant à la liste des personnes à qui Tracfin peut transmettre des informations</p>	<p>Ministère de l'intérieur et des Outre-mer, Parlement</p>	Immédiat	<p>Modification du code électoral (partie législative) et du code monétaire et financier (partie législative)</p>
32	<p>Tirer les conséquences, dans le projet de loi de finances pour 2025, de l'impact de la mise en œuvre de la loi « Ingérences étrangères » sur le budget de la Haute autorité pour la transparence de la vie publique, au regard des nouvelles missions qui lui sont confiées</p>	<p>Ministère de l'économie et des finances, Parlement</p>	2025	<p>Loi de finances pour 2025</p>
33	<p>Intégrer, dans le rapport au Parlement sur l'état de la menace liée aux ingérences étrangères prévu par la loi « Ingérences étrangères », un premier bilan du fonctionnement de la mise en œuvre du dispositif de contrôle des représentants intérêts agissant pour le compte de mandants étrangers présentant, le cas échéant, les limites rencontrées par la Haute autorité pour la transparence de la vie publique</p>	<p>Gouvernement, HATVP, Parlement</p>	2027	<p>Loi</p>

34	Défendre, au niveau européen dans le cadre de la discussion du paquet « défense de la démocratie », un niveau d'exigence en matière de transparence des activités de représentation d'intérêts exercées depuis l'étranger comparable à celui prévu par la loi « Ingérences étrangères »	Ministère de l'Europe et des affaires étrangères	Immédiat	Négociations au niveau de l'Union européenne
35	Conduire des enquêtes auprès des ministres « pressentis » pour s'assurer de l'absence d'exposition à des influences étrangères.	Président de la République, Premier ministre, Ministère de l'intérieur (DGSI)	Prochaine nomination de membres du Gouvernement	Action des services
36	Encourager résolument en tant que bonne pratique le « sourçage » des amendements et questions parlementaires présentant un lien avec une possible influence étrangère	Assemblée nationale, Sénat	Immédiat	Action du déontologue de l'Assemblée nationale, action du comité de déontologie du Sénat
Poursuivre le renforcement de la protection de l'université et de la recherche face aux opérations d'influence				
37	Mener un travail de structuration des dispositifs de détection des menaces liées aux influences étrangères au sein des établissements d'enseignement supérieur et de recherche piloté au niveau ministériel, en incluant les établissements privés	Ministère de l'enseignement supérieur et de la recherche, Service de défense et de sécurité	Lancement immédiat	Action des services
38	Poursuivre la mise en œuvre des recommandations du « rapport Gattolin », notamment en matière de la protection des sciences humaines et sociales, de contrôle des accords internationaux, et de transparence sur les liens d'intérêts des chercheurs ainsi que sur les financements extra-européens des établissements privés	Ministère de l'enseignement supérieur et de la recherche, Service de défense et de sécurité, Parlement	Immédiat	Loi, mesures réglementaires, action des services

39	Prévoir une procédure d'encadrement systématique des bourses à financement étatique ou para-étatique	Ministère de l'enseignement supérieur et de la recherche, Service de défense et de sécurité	Immédiat	Mesures réglementaires, action des services
Maintenir un niveau de vigilance élevé à l'égard des enjeux liés au financement des cultes				
40	Combler les lacunes du cadre juridique issu de la loi du 24 août 2021 confortant les principes de la République en matière de contrôle du financement étranger des cultes	Ministère de l'Intérieur, Parlement	2025	Modification de la loi du 9 décembre 1905 concernant la séparation des Églises et de l'État, modification du code monétaire et financier (partie législative)
Poser collectivement les fondations d'une véritable résilience de la société				
41	Créer, au sein de Viginum, une nouvelle fonction de sensibilisation et de formation à la sécurité informationnelle, y compris en direction des acteurs privés	SGDSN, Viginum	2025	Modification du décret n° 2021-922 du 13 juillet 2021 et du décret n° 2021-1587 du 7 décembre 2021
42	Mener une évaluation exhaustive des dispositifs français d'éducation aux médias et plus largement à l'esprit critique pour consacrer l'éducation aux médias et à l'information comme grande cause nationale, en y intégrant une dimension spécifique aux influences étrangères malveillantes	Ministère de l'éducation nationale, Clemi	Immédiat	Décision du Gouvernement
43	Créer un <i>Pass Médias</i> pour les jeunes, sur le modèle du <i>Pass Culture</i>	Ministère de l'éducation nationale, ministère de la culture, ministère de l'économie et des finances, Parlement	Immédiat	Loi de finances, arrêté ministériel
44	Intégrer dans la Journée défense et citoyenneté une dimension portant sur les influences étrangères	Ministère des armées, Parlement	Immédiat	Loi ou décret

45	Créer une spécialité de la réserve opérationnelle et de la réserve citoyenne de défense et de sécurité dédiée à la fonction d'influence et mobilisable pour la détection et la riposte aux opérations d'influence étrangères	Ministère des armées	Immédiat	Instruction
46	Sensibiliser les élus sur les enjeux liés aux influences étrangères malveillantes (commande publique, cybersécurité etc.)	Ministère de l'intérieur et des Outre-mer, Parlement	Immédiat	Loi ou décret
47	Examiner la possibilité d'habiliter au secret de la défense nationale davantage de responsables publics, en particulier les exécutifs locaux et les présidents d'établissements d'enseignement supérieur dans la limite du besoin d'en connaître	Premier ministre, SGDSN	Immédiat	Décision du Gouvernement

DOCUMENT PROVISOIRE

DOCUMENT PROVISOIRE