N° 1661

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 2 juillet 2025.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES

en conclusion des travaux d'une mission d'information
sur le thème de ***« l'opérationnalisation de la nouvelle fonction stratégique influence »***

ET PRÉSENTÉ PAR

Mmes NATALIA POUZYREFF et MARIE RÉCALDE

Députées

SOMMAIRE

—

Pages

INTRODUCTION : « GAGNER ENSEMBLE LA GUERRE DE L'INFORMATION » 9

I. FACE À L'AUGMENTATION DES MENACES DANS LE CHAMP INFORMATIONNEL, LA FRANCE S'EST DOTÉE EN 2022 D'UNE SIXIÈME FONCTION STRATÉGIQUE « INFLUENCE », QUI DEMEURE EN COURS D'OPÉRATIONNALISATION 11

A. UNE PRISE DE CONSCIENCE RÉCENTE, FORMALISÉE DANS LA REVUE NATIONALE STRATÉGIQUE DE 2022 11

1. Une menace informationnelle en pleine mutation, véritable danger pour les démocraties 11

a. Le champ informationnel : un champ de bataille à part entière 11

b. Une menace ancienne aux modes d'action renouvelés : « les habits neufs de la propagande » 13

i. Typologie des stratégies d'influence : une combinaison d'actions de court et de long termes 14

ii. L'apparition de nouveaux acteurs aux côtés des États : organisations terroristes, acteurs privés, *proxys*, sociétés militaires privées 16

iii. Une combinaison d'actions dans les champs informationnel et physique, sur le territoire national et contre les intérêts français à l'étranger 20

c. Le changement d'échelle engendré par les réseaux sociaux et le recours à l'intelligence artificielle 22

i. Le rôle de caisse de résonance jouée par les réseaux sociaux 22

ii. Une rupture qualitative et quantitative – le défi d'une forme « d'industrialisation » de la production de contenus et des modes opératoires de manipulation de l'information 24

iii. À moyen terme, l'enjeu de la corruption des intelligences artificielles 27

2. La création d'une fonction « influence » afin de faire face à l'intensité croissante de la compétition dans le champ des perceptions 28

a. La volonté affichée de sortir de la naïveté 28

b. L'influence : un concept plastique à la définition délicate 29

B. UNE FONCTION STRATÉGIQUE NECESSAIREMENT INTERMINISTÉRIELLE ET À L'ARCHITECTURE COMPLEXE, MAIS DONT LA STRUCTURATION PROGRESSE 31

1. Une organisation interministérielle en cours de consolidation 32

a. Le choix d'une approche interministérielle et multidimensionnelle : une fonction stratégique dont le chef de filât a été confié au ministère de l'Europe et des affaires étrangères 32

b. La dichotomie entre l'influence (à destination de l'international) et la lutte contre les manipulations de l'information (sur le territoire national) 37

c. Une organisation à clarifier 38

i. Une architecture complexe 38

ii. Une coordination interministérielle qui s'effectue essentiellement *via* des comités spécialisés dédiés : le comité opérationnel de lutte contre les manipulations de l'information (COLMI) et le comité « enjeux informationnels » 39

2. La structuration progressive d'une fonction « influence et lutte informationnelle » au sein des armées 40

a. La prise de conscience anticipée des armées : de la lutte informatique d'influence à la fonction « influence et lutte informationnelle » 42

i. La lutte informatique d'influence 42

ii. La doctrine ILI, déclinaison militaire de la fonction stratégique « influence » 43

b. Intégrer nativement l'influence aux opérations militaires 43

i. Le rôle central de la cellule ASO, gardienne de la cohérence d'ensemble et pilote de la déclinaison opérationnelle de la fonction ILI 44

ii. Les autres acteurs mobilisés au-delà du premier cercle 49

iii. Les principaux défis rencontrés 50

C. UNE RÉPONSE NATIONALE QUI S'INSCRIT DANS UN ÉCOSYSTÈME EUROPÉEN ET INTERNATIONAL MARQUÉ PAR LA PROFUSION DES INITIATIVES AU RISQUE DE NUIRE À LA LISIBILITÉ DE LA RÉPONSE 50

1. Une mobilisation bienvenue face à une menace qui ne connaît pas de frontières 50

a. L'Union européenne : le rôle précurseur du SEAE en matière de lutte contre les manipulations de l'information 51

b. L'OTAN : une organisation efficace qui pourrait être remise en cause par la nouvelle administration américaine 54

c. Des mécanismes internationaux nombreux 55

2. Une multiplication des concepts, des acteurs et des approches, qui nuit à la lisibilité d'ensemble de l'action menée 56

a. La nécessaire harmonisation des approches et des pratiques 56

b. L'approfondissement de la coopération en matière de contre-hybridité 57

c. Des coopérations bilatérales à renforcer 58

II. EN COMPLÉMENT DES ACTIONS D'INFLUENCE MENÉES À DESTINATION DE L'INTERNATIONAL, LA NÉCESSITÉ DE RENFORCER LA RÉSISTANCE DE LA SOCIÉTÉ FRANÇAISE FACE AUX STRATÉGIES DE DESTABILISATION MENÉES PAR NOS COMPÉTITEURS 59

A. LES LIMITES DE LA STRATÉGIE D'INFLUENCE FRANÇAISE FACE AUX ATTAQUES DÉSINHIBÉES DE NOS COMPÉTITIEURS CIBLANT LES INTÉRÊTS FRANÇAIS À L'ÉTRANGER MAIS ÉGALEMENT, DIRECTEMENT SUR LE TERRITOIRE NATIONAL 60

1. Une asymétrie assumée face à nos compétiteurs : le respect de l'État de droit et des principes démocratiques 60

a. La fragilité, voire la relative impuissance, des États démocratiques face aux stratégies de nos compétiteurs et à l'instrumentalisation des réseaux sociaux 60

b. Le piège des procès en propagande et en censure – préserver l'équilibre entre régulation et liberté d'expression 62

2. Une stratégie qui demeure essentiellement défensive, en réaction aux attaques menées par nos compétiteurs 65

a. Le rôle de VIGINUM demeure limité à la détection et à la caractérisation des ingérences numériques étrangères 65

b. Des efforts à poursuivre en matière de riposte et de réponse de court et de long termes 66

3. L'absence de vision commune et partagée affaiblit la stratégie française 68

B. DIFFUSER UNE VÉRITABLE « CULTURE DE L'INFLUENCE » FRANÇAISE AU-DELÀ DES MINISTÈRES RÉGALIENS 70

1. Élaborer une stratégie nationale d'influence globale, assumée, excédant le seul champ des armées 71

a. Le besoin d'inscrire l'influence militaire dans un narratif national global et positif 71

b. Un message unifié et mieux ciblé – le modèle britannique 72

c. Clarifier le pilotage et assumer les actions menées 75

i. Orienter et intégrer l'action des différents acteurs 75

ii. Le besoin d'une vision commune déclinable dans tous les champs de l'action publique 77

2. Concevoir une doctrine de réponse claire 79

a. Définir des seuils de réponse tout en veillant à ne pas rendre l'action prévisible . 79

b. Recourir à la déclassification de contenus de manière encadrée 81

c. Renforcer les sanctions : passer de la lutte contre les manipulations de l'information à la lutte contre les manipulateurs de l'information 82

3. Envisager l'action de manière plus offensive sans renier les valeurs démocratiques 89

4. Poser la question de l'adéquation entre les moyens et les ambitions 92

a. Des besoins humains et capacitaires 92

b. La nécessaire clarification des objectifs et la définition de priorités géographiques et thématiques 96

c. La nécessité de mieux identifier les moyens alloués à cette nouvelle fonction dans une logique de transparence 98

d. … et de mieux mesurer l'efficacité des actions menées 98

C. AGIR EN AMONT POUR RÉDUIRE LES FACTEURS STRUCTURELS DE VULNÉRABILITÉ FACE AUX MANIPULATIONS DE L'INFORMATION EN ASSOCIANT LA SOCIÉTÉ CIVILE 99

1. Renforcer l'immunité collective de la société française 99

a. Objectiver les conséquences des stratégies de désinformation sur la société française et identifier les vulnérabilités 100

b. Agir en amont pour réduire les facteurs structurels de vulnérabilités face à la désinformation 102

i. À court terme : poursuivre les actions de *pre-bunking* et de *debunking* afin de limiter l'effet des narratifs adverses 102

ii. À moyen et long termes : renforcer l'éducation aux médias et à l'esprit critique 104

c. Mieux prendre en compte les défis posés par les réseaux sociaux et les médias en matière de lutte contre la désinformation 109

i. L'enjeu de l'application du cadre juridique existant 109

ii. Redoubler de vigilance en période électorale 110

iii. L'enjeu de la préservation du modèle économique des médias traditionnels 114

iv. La piste de la certification de l'information de qualité 117

d. La société civile en première ligne 118

i. Poursuivre les efforts visant à bâtir un écosystème de confiance et à rendre les citoyens acteurs de la défense de l'espace informationnel 118

ii. Promouvoir et financer la recherche transdisciplinaire dans le champ informationnel . 122

iii. Décentraliser la politique de lutte contre les manipulations de l'information 123

2. Prendre en compte la guerre cognitive, comme une composante majeure de la guerre de demain 124

a. La perspective du cerveau humain comme champ de bataille 124

b. Engager une réflexion sur les outils de « défense psychologique » ? 126

3. Admettre que champs physiques et informationnels ne peuvent être entièrement décorrélés : « l'influence ne peut pas tout » 128

EXAMEN EN COMMISSION 129

ANNEXE I : LISTE DES PROPOSITIONS 131

ANNEXE II : AUDITIONS ET DÉPLACEMENTS DES RAPPORTEURES 137

1. Auditions 137

2. Déplacements 140

➢ Déplacement à Bruxelles (le 4 février 2025) 140
➢ Déplacement à Londres (le 10 mars 2025) 140
➢ Déplacement sur le site de VIGINUM à Paris (le 6 mai 2025) 140

INTRODUCTION : « GAGNER ENSEMBLE LA GUERRE DE L'INFORMATION »

« La guerre est acte de violence destiné à contraindre l'adversaire à notre volonté. »

Carl von Clausewitz, De la guerre (1832)

● Si la dimension psychologique a toujours été présente dans la guerre, comme en témoigne la citation de Clausewitz, les manœuvres informationnelles visent dorénavant à déstabiliser les démocraties dès le temps de paix.

Comme l'indiquait le Premier ministre, François Bayrou, dans son discours d'inauguration au Forum VIGINUM de mars 2025, *« Nous sommes en paix, et pourtant nous sommes déjà en guerre. Une guerre singulière, qui n'a ni début ni fin, qui ne se déroule ni sur terre, ni sur mer, ni dans les airs, une guerre qui pour être virtuelle ou hybride n'en est pas moins réelle : la guerre informationnelle. »*

L'enjeu est crucial puisqu'en l'absence de réponse, le risque consiste à « *être défait sans être envahi* », face aux stratégies hybrides de plus en plus désinhibées de nos compétiteurs, agissant sous le seuil de la conflictualité dans une tentative de contournement par le bas de notre dissuasion.

Si le recours à des méthodes de guerre hybride et notamment à des manœuvres informationnelles ne constitue pas une menace nouvelle, la rapidité d'exécution, l'ampleur et l'intensité de celles-ci, le sont, favorisées par l'évolution technologique rapide dans un monde interconnecté. L'ampleur des manœuvres informationnelles peut ainsi être amplifiée artificiellement par le recours aux réseaux sociaux et dorénavant à l'intelligence artificielle. De nouveaux acteurs émergent également aux côtés des États : organisation terroriste, acteurs privés, proxys, sociétés militaires privées, etc.

Ainsi, le Forum économique mondial identifiait la désinformation comme le risque global le plus important à court terme dans son rapport 2025 [(1)].

L'objectif recherché n'est pas tant de modifier les perceptions des citoyens, que d'instiller le doute généralisé pour discréditer les démocraties libérales. Les revers informationnels essuyés par l'armée française au Sahel, qui ont abouti au retrait des forces sans qu'elles n'aient véritablement perdu de combat sur le terrain, constituent un tournant dans la prise de conscience des autorités françaises.

● Aussi, vos rapporteures ont-elles cherché à déterminer la manière dont la France pouvait se protéger face à cette menace et élaborer une réponse efficace pour « gagner la guerre de l'information », sans se départir de ses valeurs démocratiques.

---

(1) 2025 Elsner, M., Atkinson, G., & Zahidi, S. (2025). Global risks report 2025 (20th ed.). World Economic Forum. (lien)

La Revue nationale stratégique de 2022 a en effet consacré la création d'une sixième fonction stratégique « Influence », témoignant d'une prise de conscience salutaire et visant à apporter une réponse face à l'augmentation des attaques informationnelles ciblant la France. Elle prévoit que la fonction stratégique s'incarnera dans une stratégie nationale d'influence qui « *fixera le cadre général de l'action de l'ensemble des acteurs concernés, déterminera les intentions et permettra d'orienter les stratégies nationales sectorielles et/ou géographiques* » Or, aucune stratégie nationale d'influence n'a été publiée à ce jour. Vos rapporteures ont donc souhaité s'assurer de la bonne opérationnalisation de la fonction influence.

Par ailleurs, vos rapporteures ont acquis la conviction qu'au-delà des actions d'influence à destination de l'international, il était essentiel de mieux se protéger au niveau national. Réduire nos vulnérabilités doit ainsi constituer un préalable. En conséquence, vos rapporteures ont fait le choix de ne pas limiter leurs travaux strictement à l'influence, au sens de communication proactive à destination de l'international et d'actions visant à modifier les perceptions, mais de s'intéresser également à la protection de notre espace informationnel vis-à-vis des stratégies d'influence étrangères. Vos rapporteures se sont ainsi attachées à évaluer la mise en œuvre de la fonction influence à l'extérieur des frontières françaises (volet proactif) et son corollaire, la lutte contre la désinformation et les manipulations de l'information sur le territoire national (volet défensif).

Au terme de six mois de travaux, marqués par plus d'une trentaine d'auditions en France et à l'étranger, vos rapporteures formulent une trentaine de propositions en vue, d'une part, de l'élaboration d'une stratégie nationale d'influence globale, excédant le seul champ des armées et, d'autre part, du renforcement de la résistance de la société française face aux stratégies de déstabilisation menées par nos compétiteurs.

I. FACE À L'AUGMENTATION DES MENACES DANS LE CHAMP INFORMATIONNEL, LA FRANCE S'EST DOTÉE EN 2022 D'UNE SIXIÈME FONCTION STRATÉGIQUE « INFLUENCE », QUI DEMEURE EN COURS D'OPÉRATIONNALISATION

La création d'une nouvelle fonction stratégique influence dans la revue nationale stratégique (RNS) de 2022 marque une prise de conscience salutaire, qui a débouché sur la structuration d'une politique interministérielle, s'inscrivant dans un cadre européen et international plus large.

A. UNE PRISE DE CONSCIENCE RÉCENTE, FORMALISÉE DANS LA REVUE NATIONALE STRATÉGIQUE DE 2022

1. Une menace informationnelle en pleine mutation, véritable danger pour les démocraties

La France doit faire face à un accroissement de la menace informationnelle. Si historiquement les attaques informationnelles ont pu se concentrer sur la présence française à l'étranger, notamment sur le continent africain, l'on observe une augmentation significative du nombre d'attaques ciblant directement le débat public numérique français. Comme le rapporte le SGDSN dans son rapport annuel d'activité 2024, « *dans un contexte de vives tensions internationales, l'année 2024 a été marquée par une augmentation significative du nombre de campagnes numériques de manipulation de l'information visant les démocraties, notamment la France* [(1)]. »

Si l'action sur les perceptions constitue une menace ancienne, presque aussi vieille que la guerre, ses modes d'actions ont été profondément renouvelés, et sa portée amplifiée par les réseaux sociaux et le recours à l'intelligence artificielle.

a. Le champ informationnel : un champ de bataille à part entière

Le champ informationnel [(2)] **constitue un champ de bataille à part entière**. Les armées définissent le champ informationnel comme étant « *à la fois l'espace dans lequel les informations circulent et un espace de confrontation militaire* [(3)]. » Le champ informationnel constitue l'un des sept milieux et champs de conflictualité (terre, mer, air, cyber, espace exo-atmosphérique, informationnel, électromagnétique) définis dans le Concept d'emploi des forces (CEF, 2020).

---

(1) Rapport d'activité 2024 – SGDSN.

(2) Le champ informationnel est un champ immatériel qui comprend l'information elle-même, ainsi que les personnes et les systèmes informatiques qui reçoivent, traitent et transmettent l'information.

(3) CICDE, Doctrine interarmées 10 – Influence et lutte informationnelle, 2023.

● **En effet, le champ informationnel est devenu le lieu où s'exerce la lutte informationnelle, voire une véritable « guerre de l'information [(1)]».** Selon l'historien David Colon [(2)], auteur de *La Guerre de l'information. Les États à la conquête de nos esprits*, la guerre informationnelle est ainsi un substitut à la guerre traditionnelle. Si elle intervient en dessous du seuil d'un conflit ouvert, il s'agit bel et bien d'un affrontement direct entre puissances dans toutes les dimensions de la sphère informationnelle. Dans un monde où l'information devait constituer un facteur d'émancipation des peuples et signer la fin des régimes autoritaires, elle est désormais une arme de ces derniers contre les régimes démocratiques, qui sont particulièrement vulnérables car ils défendent un débat public libre, le respect des libertés et la libre circulation des informations. Selon l'auteur, « *la guerre de l'information est aujourd'hui une guerre totale, qui implique toutes les dimensions de nos sociétés et de nos existences, que nous en soyons conscients ou non*. [(3)] »

Le phénomène est d'autant plus manifeste que les technologies de l'information et la numérisation des sociétés confèrent à l'information une valeur exceptionnelle dans ce que le Président de la République qualifiait déjà de « *guerre hybride mondialisée* » dans la RNS de 2022. Aussi, selon le général de division Jean-Michel Meunier, chef de la cellule anticipation stratégique et orientations (ASO) de l'État-major des armées, auditionné par vos rapporteurs, l'information est-elle à la fois le lieu de la confrontation (le champ informationnel) et l'objet de la confrontation (accéder à l'information et contrôler le champ informationnel).

● **Les manœuvres informationnelles malveillantes s'inscrivent dans le cadre plus large de stratégies hybrides, intervenant sous le seuil de la conflictualité armée et qui visent, selon le général Meunier, à « *défaire sans envahir* »,** c'est-à-dire à défaire militairement, mais surtout à défaire la société et chercher à décourager voire à démoraliser l'adversaire.

En effet, dès la phase de compétition, le champ informationnel est particulièrement propice au déploiement de stratégies hybrides. Ces dernières se définissent comme le recours par un acteur étranger à des « *combinaisons volontairement ambigües de modes d'actions directs et indirects, militaires ou non, légaux ou non, et souvent difficilement attribuables. Ces stratégies peuvent avoir des conséquences importantes pour les démocraties car elles visent à les délégitimer, affaiblir leurs forces morales et leur cohésion ou réduire leur potentiel économique et de défense nationale.* » [(4)]

Jouant avec les seuils estimés de riposte et de conflit armé, les stratégies hybrides sont conçues pour contraindre et affaiblir l'adversaire. L'effet recherché est la subversion : il s'agit de déstabiliser les institutions démocratiques pour renverser l'ordre établi, jeter le doute dans les opinions publiques voire interférer

(1) La Guerre de l'information. Les États à la conquête de nos esprits, David Colon, Paris, Tallandier, 2023.

(2) Ibid.

(3) Ibid.

(4) RNS, 2022.

dans l'organisation des processus électoraux. Menées sous le seuil du conflit armé, elles visent enfin à tester la solidité de l'article 5 et des garanties de sécurité collective dans le cadre de l'Alliance atlantique.

b. Une menace ancienne aux modes d'action renouvelés : « les habits neufs de la propagande »

● L'utilisation de stratégies indirectes et d'actions d'influence ne constitue pas en réalité un phénomène nouveau.

Les opérations de simulation, de dissimulation ou d'intoxication sont aussi vieilles que la guerre et visent à jouer sur les perceptions de l'adversaire afin de le tromper sur ses intentions, ses capacités réelles et sur sa stratégie (1).

En effet, SUN TZU considère dans son *Art de la guerre* que *« parvenir à battre son adversaire sans l'avoir affronté est la meilleure conduite »* (2). La guerre informationnelle a d'ailleurs déjà pu conduire au déclenchement de conflits, comme ce fut le cas avec l'incident de la dépêche d'Ems, qui contribua au déclenchement de la guerre franco-prussienne en 1870, ou jouer un rôle déterminant dans son évolution comme lors de la seconde guerre mondiale, à travers les opérations *Mincemeat* (1943) ou encore Fortitude (1944), visant à manipuler les perceptions et le raisonnement cognitif de l'ennemi (3). Le recours à l'arme de l'information constitue également un héritage de la guerre froide et depuis les années 1960, la notion de champ des perceptions fait partie du champ doctrinal des forces armées.

● Toutefois, la guerre informationnelle a pris une nouvelle ampleur à l'ère des nouvelles technologies et les réseaux sociaux.

La France est depuis plusieurs années la cible d'attaques informationnelles menées par ou impliquant des acteurs étrangers. La première ingérence numérique étrangère d'ampleur documentée est l'affaire dite des « *Macron Leaks* » lors de la campagne présidentielle de 2017, que les autorités françaises ont attribuée officiellement en avril 2025 aux services de renseignement russes (GRU) à travers le mode opératoire APT 28 (*Advanced Persistent Threat*) pour son volet cyber.

Ainsi, l'on constate actuellement une augmentation des manœuvres informationnelles hostiles. La France constitue une cible privilégiée. Elle est, après l'Ukraine, le pays le plus visé en Europe par des tentatives de manipulations venant de l'étranger, notamment de Chine et de Russie, selon le rapport publié en mars 2025 par le Service européen pour l'action extérieure (4). Sur les 505 incidents relevés en Europe entre 2023 et 2024, 257 concernaient l'Ukraine, 152 visaient la France. Les Jeux olympiques et paralympiques de Paris 2024 et les élections

---

(1) Les nouvelles formes de guerre, Le Rubicon, Colonel David Pappalardo, « la guerre cognitive : agir sur le cerveau de l'adversaire ».

(2) Sun Tzu, L'art de la guerre.

(3) Bettina TRABELSI, Assistante de recherche à l'observatoire des conflits (PEP/Observatoire des conflits). (lien).

(4) 3rd EEAS Report on Foreign Information Manipulation and Interference Threats, SEAE, mars 2025. (lien).

législatives en constituaient les principales cibles. Depuis le mois de juin 2023, VIGINUM a directement contribué à révéler publiquement plusieurs campagnes de manipulation de l'information impliquant des acteurs étrangers et susceptibles de porter atteinte aux intérêts fondamentaux de la Nation, dont le réseau « RRN », l'opération dite des « étoiles de David », la campagne de dénigrement des Jeux olympiques (JO) baptisée « *Olimpiya* », le dispositif « *Portal Kombat* », ou encore le faux site de recrutement pour l'armée de Terre « s'engager-Ukraine ».

i. Typologie des stratégies d'influence : une combinaison d'actions de court et de long termes

● Les stratégies d'influence de nos compétiteurs reposent sur une combinaison d'action de court et de long termes.

Selon le chef d'état-major des armées (CEMA), le général d'armée Thierry Burkhard, « *Le véritable paramètre discriminant et contraignant des actions d'influence est cependant d'ordre temporel. De façon générale, même si elle demande aussi de la réactivité, l'influence est une action du temps long qui nécessite une vision stratégique stable.* » (1) Des actions de court et de long termes coexistent néanmoins, les unes pouvant nourrir les autres. Selon la chercheuse Christine Dugoin-Clément (2), auditionnée par vos rapporteures, une fois devenus familiers, les narratifs promus par un acteur étranger pourront être « réactivés », conformément aux concepts de « *shaping* » ou de « *framing* » qui visent à formater les perceptions sur le long terme.

● Les stratégies d'influence combinent des actions en temps de guerre mais également certaines, plus insidieuses, dès le temps de paix, afin d'affaiblir les capacités de réaction et de résistance d'un adversaire sur le plus long terme, sans avoir à recourir à la force. En effet, selon le CEMA, « *La compétition, là où se joue « la guerre avant la guerre », est le théâtre par excellence de l'influence qui trouve une place majeure dans les stratégies hybrides* (3). »

En guise d'illustration, selon le général de division Jean-Michel Meunier, chef de la cellule ASO, la Chine mène une stratégie particulièrement déstabilisatrice à l'encontre de Taïwan en la matière : « *une partie de la population taïwanaise a révélé qu'elle ne se battrait pas en cas d'invasion chinoise, parce que selon elle, les Chinois sont sympathiques sur l'application Tik Tok* (4). »

De la même manière, Christine Dugoin-Clément, auditionnée par vos rapporteures a notamment mis en lumière « l'arsenalisation » de jeux vidéo, utilisés pour formater les opinions des publics jeunes. Par exemple, la Russie utilise les jeux

---

(1) Burkhard, T. (2023). Pas de stratégie sans influence, pas d'influence sans stratégie. Revue Défense Nationale, 856(1), 9-15. (lien).

(2) Christine Dugoin-Clément, Géopolitique de l'ingérence russe, PUF, mars 2025.

(3) Burkhard, T. (2023). Pas de stratégie sans influence, pas d'influence sans stratégie. Revue Défense Nationale, 856(1), 9-15. (lien).

(4) Esprit de défense n° 14, hiver 2025 p.32.

vidéo en ligne pour exercer son influence et façonner des récits antioccidentaux, en particulier sur le continent africain. À titre d'exemple, le jeu en ligne de conception russe « *African Dawn* » développé par *African Initiative – une agence de presse russe, considérée par VIGINUM comme l'un des principaux vecteurs de la réarticulation du dispositif d'influence de la Russie en Afrique post-Prigojine* – viserait directement les jeunes Burkinabès. Le jeu, qui met en scène le coup d'État de septembre 2022 au Burkina Faso, ferait également la promotion de la méfiance envers les « forces néocoloniales », notamment la France au Sahel et représenterait opportunément la Russie et ses alliés comme des sauveurs.

● **Ces stratégies poursuivent plusieurs types d'objectifs.** Lors de son audition, M. Laurent Cordonnier, a ainsi mis en avant trois principaux effets recherchés pas les stratégies d'influence.

D'une part, il s'agit des « effets de propagande », dont la visée est de modifier les perceptions. Il s'agit d'instiller un doute sur une croyance que l'on a sur un sujet, de changer une croyance, ou d'en acquérir une nouvelle, voire de provoquer un changement de comportement, comme se mettre à partager des éléments sur les réseaux sociaux, participer à des manifestations jusqu'à un enrôlement, etc.

D'autre part, les effets recherchés consistent le plus souvent en une simple polarisation dans le but d'appuyer sur des failles qui parcourent la société ciblée et ainsi affaiblir les démocraties. Il s'agit de rendre saillante une fracture préexistante et d'augmenter la polarisation affective jusqu'à provoquer un changement de comportement. L'on peut par exemple citer, l'opération ayant consisté à imposer des étoiles de David dans les rues de Paris, instrumentalisant une fracture existante relative à l'antisémitisme, amplifiée ensuite via les réseaux sociaux.

Enfin, les stratégies cherchent *in fine* à instaurer un doute généralisé dans l'information et une baisse de confiance dans les institutions dans une forme de « stratégie du chaos » théorisée par les responsables russes [(1)]. Le défi est d'autant plus grand que certaines stratégies de manipulations de l'information ne reposent pas uniquement sur des informations fausses, mais instrumentalisent la vérité. L'on peut ainsi citer l'instrumentalisation du phénomène des punaises de lit pendant les Jeux olympiques et paralympiques de 2024, dénoncée par VIGINUM.

(1) Christine Dugoin-Clément.

ii. L’apparition de nouveaux acteurs aux côtés des États : organisations terroristes, acteurs privés, *proxys*, sociétés militaires privées

Les manœuvres informationnelles sont le fruit d’une diversité d’acteurs : aux côtés d’États, interviennent également des organisations terroristes, des proxys ou encore des acteurs privés, telles que les sociétés militaires privées. La France est à la fois ciblée sur le territoire national et à l’étranger.

● **Parmi les menaces d’origine étatiques, il ressort des auditions de vos rapporteures, que la menace russe s’avère prégnante et s’est intensifiée à mesure que la France renforçait son soutien à l’Ukraine.** Cet accroissement procède également d’une désinhibition de plus en plus forte dans le domaine hybride, qui se traduit par la multiplication des attaques par des acteurs russes ou agissant pour les intérêts de la Russie. Dans un rapport de mai 2025, VIGINUM indique ainsi avoir identifié 77 opérations de désinformation russes entre 2023 et 2025 menées dans le cadre du seul mode opératoire « Storm-1516 » (1) et visant les espaces informationnels français et européens.

De la même manière, le mode opératoire de grande ampleur « RRN » mis à jour par VIGINUM en 2023 peut également être cité pour son caractère persistant mais également pour le recours à différents modes opératoires, notamment le recours à la technique dite du « *typosquatting.* » Intitulé RRN pour *reliable recent news*, le réseau a permis d’usurper l’identité de sites internet et de médias traditionnels français mais aussi gouvernementaux pour diffuser des informations pro-russes. Une réplique du journal Le Monde ou encore du site du Ministère de l’Europe et des affaires étrangères a ainsi été créée. Les armées ont également été victimes d’un faux portail de recrutement le 15 mars 2024, reprenant la charte graphique de l’armée de Terre et proposant de s’engager en Ukraine (2).

(1) VIGINUM, Analyse du mode opératoire informationnel russe Storm-1516, mai 2025.

(2) VIGINUM, RRN : une campagne numérique de manipulation de l’information complexe et persistante, 13 juin 2023.

Synthèse - RRN : une campagne numérique de manipulation de l'information complexe et persistante

VIGINUM a identifié une campagne numérique de manipulation de l'information ayant visé plusieurs États européens depuis septembre 2022, dont la France.

Cette campagne de manipulation de l'information, suivie depuis plus d'un an par VIGINUM, a pour objectif de discréditer le soutien occidental à l'Ukraine. Dénommée *RRN* en raison de la place centrale occupée par le « média » *Reliable Recent News*, cette campagne s'articule autour de quatre composantes :

– La diffusion de contenus pro-russes liés à la guerre en Ukraine, dénigrant notamment ses dirigeants ;

– L'usurpation de l'identité de sites de médias, mais aussi gouvernementaux, européens, via la technique de *typosquatting* visant à reproduire leur nom de domaine ;

– La création de sites web d'actualités francophones partageant des contenus polémiques, instrumentalisant l'actualité nationale française ;

– La mise en œuvre de moyens inauthentiques combinés, tels que des faux sites ou des faux comptes sur les réseaux sociaux, permettant de relayer les contenus.

Pour ce faire, la campagne *RRN* s'appuie sur un ensemble de narratifs inauthentiques, reprenant quatre thèmes principaux, visant à désolidariser la société civile des instances gouvernantes :

– L'inefficacité supposée des sanctions visant la Russie, qui pèseraient avant tout sur les États européens et / ou leurs citoyens ;

– La prétendue russophobie des États occidentaux ;

– La barbarie dont feraient preuve les forces armées ukrainiennes, ainsi que l'idéologie néo-nazie qui prédominerait chez les dirigeants ukrainiens ;

– Les effets négatifs qu'entrainerait l'accueil de refugiés ukrainiens pour les États européens.

Alors que 355 noms de domaine usurpant l'identité de médias ont été détectés par VIGINUM, quatre ciblent plus spécifiquement le public francophone et reprennent l'identité graphique de quotidiens français, à savoir *20 Minutes*, *Le Monde*, *Le Parisien* et *Le Figaro*. Ce sont au moins 58 articles qui ont été publiés *via* ces canaux.

VIGINUM, dans le cadre de son investigation en sources ouvertes, a par ailleurs pu identifier l'implication d'individus russes ou russophones ainsi que celle de plusieurs sociétés russes.

À partir de la fin du mois de mai 2023, la campagne *RRN* a connu un développement inédit, puisque c'est l'identité du site web du ministère de l'Europe et des affaires étrangères qui a été usurpée.

Source : VIGINUM, synthèse du rapport RRN : une campagne numérique de manipulation de l'information complexe et persistante, 13 juin 2023.

● Si la Russie mène de nombreuses attaques particulièrement visibles, celles-ci ne doivent pas masquer les comportements d'autres compétiteurs, peut-être moins visibles mais tout aussi néfastes.

● **D’autres compétiteurs développent des stratégies de plus en plus offensives.** Des États comme l’Azerbaïdjan, la Chine, ou encore les juntes sahéliennes peuvent également avoir recours à des communications officielles agressives, des opérations clandestines de manipulation de l’information et à l’amplification artificielle de contenus sur les réseaux sociaux.

Ainsi, les campagnes informationnelles hostiles ne touchent pas nécessairement l’ensemble du territoire national de manière uniforme. Dans le rapport *UN-notorious BIG* paru en décembre 2024 (1), VIGINUM met en lumière une campagne numérique de manipulation de l’information ciblant les DROM-COM et la Corse, reflet de la volonté d’un acteur étranger d’exploiter de manière opportuniste des fractures existantes dans la société française. Cette campagne a été attribuée au *Baku Initiative Group (BIG)*, un organisme de propagande d’État, basé en Azerbaïdjan, qui tente de remettre en cause la souveraineté de la France dans les territoires d’outre-mer.

S’agissant de la Chine, Paul Charon, directeur du domaine Influence et Renseignement de l’IRSEM et auteur avec Jean-Baptiste Jeangène Vilmer, de l’ouvrage *Les Opérations d'influence chinoises. Un moment machiavélien* (Équateurs, 2024), indique avoir observé le passage d'opérations ponctuelles à de plus en plus d'opérations de long terme. La Chine dispose de moyens particulièrement développés : l’Armée populaire de libération (APL) s’est ainsi dotée d’une « Force de soutien stratégique » dédiée, incluant la base 311, dont l’appellation est littéralement : « base de la guerre de l’opinion publique, de la guerre psychologique et de la guerre du droit » (2). La démarche chinoise suivrait néanmoins davantage une « logique bureaucratique », d’abord quantitative et non qualitative. Les opérations menées, aussi complexes soient-elles, paraîtraient souvent entachées d’erreurs grossières, réduisant certainement leur impact. Une autre particularité résiderait dans le fait que l'influence chinoise demeurerait caractérisée par des actions à dominante physiques (répression transnationale, espionnage industriel, etc.) ou toponymiques (son combat le plus visible constitue le changement de nom de Pékin pour Beijing et du Tibet pour Xizang).

Enfin, les stratégies de désinformation agressives à l’encontre des intérêts français trouvent particulièrement à s’exprimer sur le continent africain, notamment au Sahel, à l’image de l’affaire dite du « charnier de Gossi », orchestrée avec l’aide des mercenaires de Wagner et visant à discréditer l’action des armées françaises au Mali en 2022. Par ailleurs, un autre exemple consiste le 28 août 2023, en la détection d’un faux ordre d’opération attribué à la France, laissant entendre que les armées françaises planifieraient avec la CEDEAO une manœuvre militaire contre le Niger, suite au coup d’État de la junte. Le document circule rapidement sur les réseaux sociaux au sein de sphères panafricanistes et pro-russes, sans pour autant atteindre les grands médias nigériens. Néanmoins, le document comporte de nombreuses

---

(1) VIGINUM, UN-notorious BIG, Une campagne numérique de manipulation de l’information ciblant les DROM-COM et la Corse, décembre 2024.

(2) Charon Paul et Jeangène Vilmer Jean-Baptiste, Les opérations d’influence chinoises – Un moment machiavélien (2e édition), Institut de recherche stratégique de l’École militaire (Irsem), octobre 2021. (lien).

erreurs permettant de montrer qu'il s'agit d'un faux (mauvaise classification, mention d'un régiment qui n'existe pas, etc.). Il contient, par ailleurs, des éléments permettant de remonter jusqu'à son auteur et au lieu de production : le document a été créé dans le fuseau GMT+4, dans lequel sont situés plusieurs oblasts russes. Une fois le document détecté, il a rapidement été identifié et dénoncé comme faux sur les réseaux sociaux par des *fact-checkers*.

● **Aux côtés des actions étatiques, plus traditionnelles, une forme de privatisation de l'influence et des stratégies de désinformation peut être constatée**.

Outre des opérateurs clairement liés aux États compétiteurs, les opérations d'influence peuvent être menées par des acteurs non officiels, rendant ainsi l'attribution plus complexe. Le recours à des « *proxies* » comme des milices privées, sont autant de moyens détournés qui rendent l'attribution des manœuvres informationnelles plus difficile. Elles offrent à la fois une forme d'agilité dans l'action, une possibilité de déni plausible pour les États commanditaires et une véritable capacité d'actions de terrain.

Depuis 2018 et l'implantation de la société Wagner sur le continent africain, les armées ont été ciblées par de nombreuses campagnes de désinformation, visant l'opération Barkhane et la présence militaire française en Afrique. Selon les informations fournies à vos rapporteures, ces manœuvres sont complexes, mobilisant à la fois des médias d'État russes (*Sputnik* et *RT* en français ne sont plus accessibles depuis l'Europe mais continuent à être suivis en Afrique), des médias privés appartenant à *Patriot Media Group*, constellation de médias appartenant anciennement à Evgueni Prigogine, et des médias et influenceurs africains, notamment panafricanistes, dont les intérêts convergent avec ceux de la Russie. Les actions d'influence russes combinent fréquemment le recours à des médias publics et des faux comptes sur les réseaux sociaux, agissant de manière synchronisée. Selon les informations fournies à vos rapporteures, le COMCYBER observe ainsi la diffusion dans la sphère informationnelle d'informations par des comptes inauthentiques, qui sont reprises par des médias publics russes. Le recours à des prestataires et influenceurs locaux est également une constante de l'action russe en Afrique, leur permettant de toucher plus facilement les audiences locales.

Selon Christine Dugoin-Clément, dans l'ouvrage précité, ces stratégies visent plusieurs cibles, y compris les opinions publiques nationales des compétiteurs auteurs des déstabilisations dans l'objectif de conforter un narratif interne. Certains contenus ciblent directement les enfants. Pour l'illustration des contenus narratifs diffusés par Wagner, selon les informations fournies à vos rapporteures, on retrouve par exemple durant la période 2019-2023, des dessins animés dénigrant la France – *par exemple, « LionBear » diffusé en Centrafrique ou « Rat Emmanuel » –*, deux films de cinéma projetés dans les villages – *the Tourist –*, ou encore deux chansons et une bande dessinée distribuées aux enfants des écoles près de Bangui. Comme le résume Christine Dugoin Clément, *« ceux qui mettent en place des opérations d'influence à des fins d'ingérence l'ont bien compris : mobiliser une multitude de*

canaux et adapter le niveau de langage ainsi que le narratif permet de travailler de manière quasi simultanée les différents niveaux de la population et de décupler l'effet recherché. » (1)

Des entreprises spécialisées offrent également leurs services et fournissent des outils inspirés du marketing stratégique, permettant de créer des contenus de désinformation, puis de les amplifier artificiellement. Auditionné par vos rapporteurs, le chercheur Maxime Audinet, auteur d'*Un média d'influence d'État. Enquête sur la chaîne russe RT* (INA, 2021), relève ainsi une tendance croissante du Kremlin à déléguer ses opérations d'influence à des acteurs privés ou semi-privés, ce qu'il qualifie « *d'ad-hocratie* ».

En dehors du cas russe, l'existence de la « *Team Jorge* », société israélienne, ancien sous-traitant de Cambridge Analytica, a par exemple, été mise en lumière par le collectif de journalistes d'investigation du consortium *Forbidden Stories* (2) dans le cadre du projet « *Story Killers* » consacré à la désinformation. La société serait impliquée dans la manipulation d'élections à grande échelle et dans le piratage de comptes de responsables politiques, notamment africains.

En revanche, sur le plan informationnel, la menace terroriste semble avoir diminué depuis la chute de l'État islamique, en particulier la production de contenus francophones, qui est maintenant très minoritaire. Les contenus de propagande sont, de plus, cantonnés à des vecteurs de diffusion fermés – *groupes privés sur Telegram, par exemple* – ce qui diminue d'autant leur visibilité. Cela ne doit pas pour autant conduire à minimiser cette menace, qui reste active et que les services continuent d'observer et de suivre.

iii. Une combinaison d'actions dans les champs informationnel et physique, sur le territoire national et contre les intérêts français à l'étranger

Les stratégies d'influence ne se limitent pas au champ informationnel et tendent à se caractériser par une combinaison d'actions dans les champs informationnel et physique.

● Les stratégies d'influence les plus sophistiquées tendent à casser la frontière entre les mondes réel et virtuel et ne doivent pas être uniquement appréciées sous le prisme numérique car elles sont également susceptibles de produire des effets dans le champ physique. S'il était courant de penser les actions d'ingérences comme venant uniquement du monde numérique et ne touchant que les perceptions, certaines stratégies hybrides mêlent des éléments cinétiques et non cinétiques, inspirées des « mesures actives » du KGB issues de la guerre froide.

---

(1) Christine Dugoin-Clément, Géopolitique de l'ingérence russe, PUF, mars 2025.

(2)Cécile Andrzejewski, Story Killers, Forbidden Stories, « Team Jorge » : Révélations sur les manipulations d'une officine de désinformation », février 2023. (lien).

● **La France a été la cible d'actions physiques sur son territoire national, amplifiées ensuite dans le champ informationnel, notamment sur les réseaux sociaux** - *qu'il s'agisse de l'affaire dite « des étoiles de David », au mois d'octobre 2023 ; des mains rouges sur le mémorial de la Shoah, peintes dans la nuit du 13 au 14 mai 2024 ou de cinq cercueils de taille réelle déposés aux abords de la Tour Eiffel le 1er juin 2024, recouverts d'un drapeau français et de l'inscription « soldats français de l'Ukraine »*. Il s'agit d'actions d'ingérence qui ont vocation ensuite à connaître un écho dans le champ informationnel, pour mieux atteindre leur but qui est de déstabiliser la société française.

Pour être efficaces et reprises, voire devenir virales dans le monde virtuel, ces manœuvres informationnelles supposent de bien connaître la société cible afin d'exploiter ses failles. Dans le cas des étoiles de David apposées dans les rues de Paris, il s'agit d'une exploitation opportuniste de l'antisémitisme, abondamment reprise dans les médias et contribuant ainsi à lui conférer la visibilité souhaitée (1).

Ces actions d'influence « hybrides » passent également par le recrutement d'agents d'influence dans le monde physique. Le documentaire « La Fabrique du Mensonge : sur la piste des agents de Poutine », réalisé par Elsa Guiol, le montre ainsi assez clairement. L'expulsion des agents et diplomates russes par les États européens a conduit au recrutement de profils moins identifiables, qualifiés de « *clearskin* » ou « d'agents jetables ». Le recrutement s'effectue dans les pays comme la Moldavie ou la Bulgarie, à moindre coût, souvent pas le biais de boucles de messagerie fermées comme Télégram.

● **À l'inverse, une campagne de manipulation de l'information peut produire des effets concrets dans le champ physique**.

L'on peut par exemple citer l'exemple du convoi de l'opération militaire « Voie sacrée ». En novembre 2021, à Kaya au Nord du Burkina Faso, des manifestants ont bloqué la route pour empêcher le passage d'un convoi de ravitaillement de l'opération Barkhane destiné à la base de Gao au Mali car les manifestants étaient persuadés que le convoi transportait des armes destinées aux djihadistes (2).

Enfin, selon les informations fournies par VIGINUM, certaines manifestations anti-occidentales en Afrique ont également été amplifiées par des appels à la mobilisation en ligne relayés de manière artificielle ou inauthentique dans le cadre de manœuvres informationnelles.

---

(1) Christine Dugoin-Clément, Géopolitique de l'ingérence russe, PUF, mars 2025.

(2) Esprit de défense n° 14, hiver 2025 p.30.

c. Le changement d'échelle engendré par les réseaux sociaux et le recours à l'intelligence artificielle

Au-delà de l'intensification de la menace, le développement des nouvelles technologies de l'information et, maintenant de l'intelligence artificielle (IA) [(1)], permet d'amplifier à moindre coût les campagnes de manipulations de l'information.

L'utilisation croissante de l'IA par des acteurs malveillants et son perfectionnement représentent, en particulier, un défi considérable pour la lutte contre les manipulations de l'information : d'une part, du fait du changement d'échelle engendré et, d'autre part, du risque à moyen terme de corruption des IA. Par sa capacité à générer du contenu faux crédible, l'IA fait ainsi peser le risque d'un scepticisme généralisé du public à l'égard de l'authenticité de tout type de contenu en ligne. Si l'authenticité devenait plus facilement contestable, le rapport à la réalité pourrait s'en trouver profondément altéré. Cette élévation de la qualité des contenus posera rapidement le défi de la capacité du citoyen à pouvoir distinguer l'authentique du synthétique.

i. Le rôle de caisse de résonance jouée par les réseaux sociaux

Les campagnes de manipulations de l'information trouvent particulièrement à s'exprimer sur les réseaux sociaux, qui permettent d'amplifier leur portée.

● Ces derniers permettent d'abord de renseigner de potentiels compétiteurs sur les lignes de fracture existantes, voire de s'insinuer dans le débat public et de cibler la cohésion d'une société. Tout citoyen devient ainsi une cible potentielle. En retour, tout citoyen devient aussi un acteur de l'influence car il dispose des outils pour retransmettre des messages. Il participe alors et démultiplie l'opération d'influence, parfois à son insu.

● Les nombreux rapports élaborés par VIGINUM éclairent les modes opératoires adverses et leur capacité à manipuler les opinions publiques au travers de relais d'amplification inauthentiques.

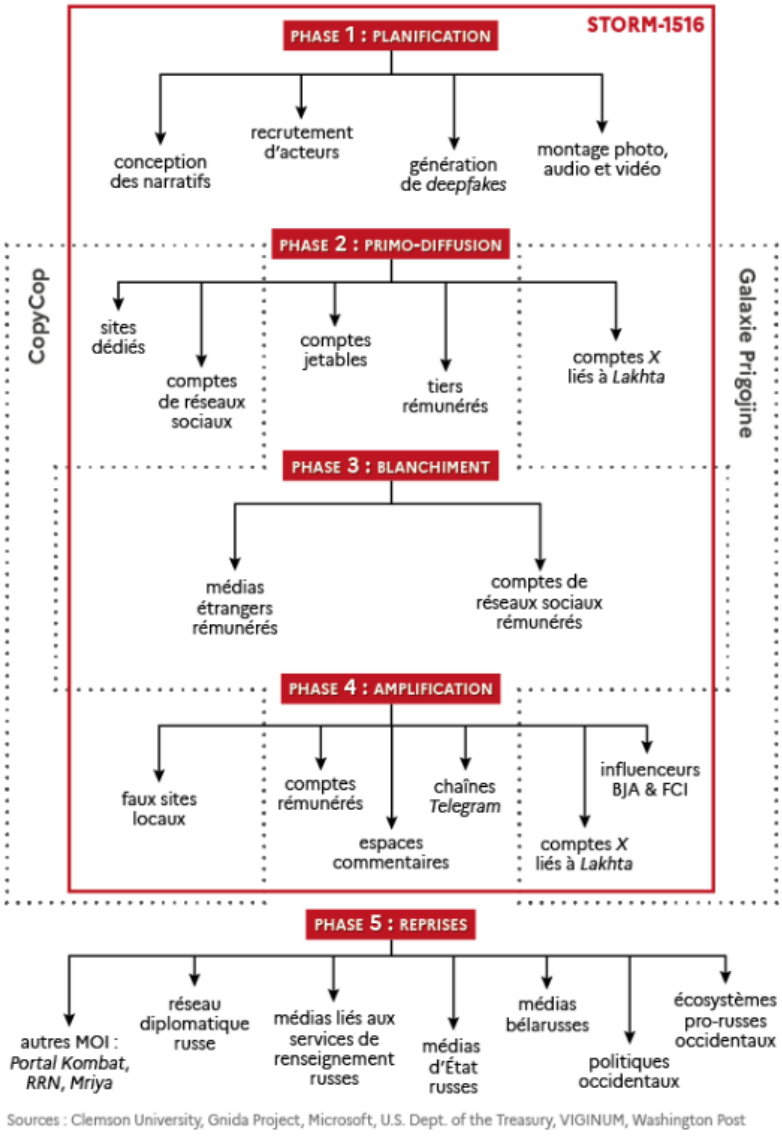
Ainsi, dans son rapport d'activité annuel de 2024, le SGDSN rapporte la manière dont VIGINUM a observé une profonde mutation des opérations d'ingérences numériques étrangères. « *Ces manœuvres informationnelles se déploient sur des plateformes où elles peuvent être amplifiées du fait de la faiblesse de la modération et le développement de nouveaux vecteurs technologiques. Les acteurs de la menace informationnelle y font usage de procédés novateurs et très diversifiés comme l'usurpation d'identité visuelle* (typosquatting), *le ciblage des*

(1) L'intelligence artificielle (IA) désigne l'ensemble des procédés logiques et automatisés, reposant généralement sur des algorithmes, destinés à reproduire, au moins partiellement, des comportements humains, tels que l'apprentissage, le raisonnement, la planification ou la création.

fact-checkers *à des fins de déstabilisation, la création de fausses vidéos ou de faux contenus par des intelligences artificielles.* »

Par exemple, comme le documente VIGINUM, le schéma de diffusion du mode opératoire Storm-1516 est particulièrement complexe et a évolué au fil du temps. Il se caractérise par la primo-diffusion de contenus par des comptes « jetables » maîtrisés par les opérateurs, ou *via* des comptes rémunérés, éventuellement appuyés par le blanchiment du narratif par l'intermédiaire de médias étrangers. Les faux récits sont ensuite amplifiés par un réseau d'acteurs pro-russes et par d'autres mode opératoires informationnels (1).

Schéma de diffusion employé par Storm-1516



Source : VIGINUM

(1) Analyse du mode opératoire informationnel russe : Storm1516, VIGINUM, mai 2025.

ii. Une rupture qualitative et quantitative – le défi d'une forme « d'industrialisation » de la production de contenus et des modes opératoires de manipulation de l'information

La démocratisation des outils d'IA générative et le rôle majeur joué par les réseaux sociaux ont contribué à un véritable changement d'échelle, amplifiant les stratégies de désinformation.

Comme le rapporte VIGINUM (1), bien que les exemples documentés en sources ouvertes tendent à démontrer que l'usage de l'IA ne permet pas, pour le moment, d'augmenter drastiquement l'impact d'une stratégie de manipulation de l'information, le recours croissant à cette technologie permet d'accroître la réactivité des acteurs malveillants, ainsi que d'augmenter l'échelle de leurs actions.

Depuis deux ans, VIGINUM observe un recours croissant à l'IA générative qui semble principalement être utilisée au profit de trois usages malveillants :

– La création de contenus faux plus crédibles à l'aide d'outils d'IA disponibles en sources ouvertes ;

– La création et l'animation de comptes inauthentiques par des outils d'IA, capables de reproduire des comportements humains ;

– La diffusion massive, à vocation multi-plateformes et multilingue, de contenus manipulés.

Toutefois, selon les informations fournies à vos rapporteures, VIGINUM considère en effet que la démocratisation de l'usage des solutions d'IA générative ne constitue à date qu'une évolution modérée de la menace, et ce pour deux raisons principales :

– d'une part, la qualité des contenus générés ne présume pas nécessairement de leur impact sur les audiences visées, certaines recherches tendant à indiquer que des contenus exploitant des méthodes moins sophistiquées (« *cheapfakes* ») peuvent être aussi nuisibles que des contenus synthétiques sophistiqués. À titre d'exemple, de vraies images, non générées par IA, mais instrumentalisées ou sorties de leur contexte dans le cadre de manœuvres malveillantes, peuvent avoir un impact important, à l'image des étoiles de David.

– d'autre part, si l'IA générative permet d'accélérer les capacités de production et de dissémination de contenus des acteurs de la menace et d'abaisser les coûts associés, elle ne permet pas, à ce stade, de faciliter leur distribution et leur viralité auprès d'audiences cibles, ce qui demeure le principal défi des manœuvres informationnelles.

---

(1) VIGINUM, Enjeux systémiques - Défis et opportunités de l'intelligence artificielle dans la lutte contre les manipulations de l'information, février 2025.

● L’IA permet des gains de productivité qui ont fait passer les opérations d’influence à une nouvelle échelle.

Parce qu’elle est capable de produire en grande quantité des contenus (textes, vidéos, images) de bonne qualité pour un moindre coût, l’IA générative permet aux acteurs malveillants de toucher à la fois un public le plus large possible, mais également s’ils le souhaitent, de cibler très précisément certains individus avec des contenus sophistiqués et ciblés (facilité de traduction des contenus textuels, par exemple). Ainsi, les outils de grand modèle de langage (LLM) comme ChatGPT permettent de générer un discours crédible et adapté à l’audience cible. Les outils d’IA permettront de dépasser le simple « bot » préprogrammé mais incapable de varier ses actions, en insérant de l’aléa et de l’adaptation. La production de contenus par l'IA se développe rapidement et va massifier les campagnes d'information, tout en les rendant moins détectables, les outils LLM étant en mesure de faire varier le texte pour délivrer un même message.

De plus, la massification de ces contenus assure un impact à court et long termes, car ces contenus attirent l’attention et suscitent l’engagement sur le moment, mais aussi parce qu’ils saturent complétement le champ informationnel, ce qui ancre leurs narratifs erronés dans la durée.

Auditionnée par vos rapporteurs, Chine Labbé, fondatrice de Newsguard, s’est déclarée inquiète de la sophistication croissante des campagnes de manipulation de l’information qui s’appuient sur des *deepfakes* ou hypertrucages de qualité de plus en plus grande, rendant plus difficile leur détection. Ainsi, 5 000 électeurs du New Hampshire ont reçu lors des primaires démocrates américaines en janvier 2024 un faux appel téléphonique du candidat Joe Biden leur demandant de ne pas rendre aux urnes, au prétexte que « *voter ce mardi ne fera qu’aider les Républicains à faire réélire Donald Trump* [(1)] ». Par ailleurs, selon le SEAE, dans le rapport de VIGINUM précité, une récente opération informationnelle ayant ciblé l'élection présidentielle et le référendum d’adhésion à l'UE en Moldavie a été mise en lumière. Dans ce cas précis, un contenu généré par l'IA et un logiciel dédié ont été utilisés pour tenter de tromper les électeurs, et d’influencer leur perception de l'adhésion à l'UE et de la candidate à la présidence Maia SANDU. Ainsi, au début du mois d'octobre 2024, une vidéo générée par l'IA et contenant une imitation de la voix de la présidente de la Moldavie a été diffusée sur Telegram et TikTok. Ce contenu *deepfake* prétendait que l'adhésion de la Moldavie à l’UE obligerait le pays à adopter des lois concernant la communauté LGBTQ+, ou encore à vendre des terres nationales à des étrangers européens.

● En plus des capacités de production de contenus décuplées, le recours à l’IA couplée à l’utilisation des réseaux sociaux contribue également à une plus grande automatisation de la diffusion des contenus potentiellement trompeurs.

---

(1) Esprit de défense n° 14, hiver 2025, p. 32.

L'IA est notamment utilisée dans la **mise en place d'actions coordonnées** dans un laps de temps très court, sur plusieurs plateformes et dans de nombreuses langues**.** À titre d'exemple, Newsguard a identifié 1 150 sites web d'information, entièrement ou principalement générés par des modèles de langage d'IA dans un total de 16 langues différentes (1). Comme le rappelle VIGINUM dans le rapport précité, au-delà du fait que ces sites constituent des dispositifs pré-positionnés susceptibles d'être activés dans le cadre de manœuvres informationnelles, ils permettent également à leurs opérateurs de capter de grands volumes d'investissements publicitaires programmatiques au détriment de médias authentiques.

Enfin, l'IA est utilisée pour la création et la gestion de faux comptes qui constituent des relais de ces campagnes de désinformation.

Comme le rappelle le sociologue Gérald Bronner, dans *Apocalypse cognitive* (2021), le coût nécessaire pour démentir une fausse information est bien supérieur à celui nécessaire pour en produire une. *In fine,* la méfiance induite vis-à-vis de l'information pourrait ensuite être exploitée par des acteurs malveillants, comme l'ont théorisé des chercheurs de l'université de Yale (2) aux États-Unis à travers le concept de « dividende du menteur ». Plus une société apprend à être sceptique, plus il devient facile pour un menteur de remettre en question des faits pourtant irréfutables, ce qui pourrait à terme déstabiliser en profondeur les processus démocratiques selon VIGINUM (3).

● Toutefois, l'IA elle-même peut représenter une solution efficace pour renforcer la lutte contre les manipulations de l'information, que ce soit pour analyser des données massives et variées ou pour détecter des comportements inauthentiques.

Les capacités d'analyse de données massives offertes par l'IA améliorent qualitativement et quantitativement les capacités d'analyse sur les réseaux sociaux. L'IA améliorera également les outils de détection des comportements inauthentiques, par exemple, en réduisant le temps nécessaire à l'identification d'une campagne ou en détectant une vidéo hypertruquée.

Lors du Sommet pour l'intelligence artificielle qui s'est tenu les 10 et 11 février 2025, VIGINUM a annoncé avoir développé des outils au bénéfice de la société civile pour aider à mieux détecter certains procédés utilisés pour mettre en œuvre des ingérences numériques étrangères en s'appuyant sur l'IA comme le « méta détecteur de contenus artificiels ». Les agents du Datalab de VIGINUM mobilisent l'IA à la fois pour faciliter l'exploration des données et pour identifier

---

(1) Newsguard AI Tracking Center, consulté le 7 janvier 2025. (lien).

(2) Kaylyn Jackson Schiff, Daniel Schiff, and Natalia S. Bueno, 2024, « The Liar's Dividend: Can Politicians Claim Misinformation to Evade Accountability? », American Political Science Review, (lien), cité par VIGINUM.

(3) Enjeux systémiques - février 2025 – Défis et opportunités de l'intelligence artificielle dans la lutte contre les manipulations de l'information, VIGINUM.

des marqueurs d'inauthenticité, afin de caractériser une ingérence numérique étrangère.

Enfin, l'IA pourrait également servir à proposer immédiatement des contre-narratifs et à traduire ceux-ci dans toutes les langues pour s'adresser dans la langue des populations victimes d'une manipulation. Il ne s'agit pas de confier à l'IA le soin de produire et diffuser automatiquement des narratifs, mais de permettre à la technologie d'assister l'action de l'homme.

iii. À moyen terme, l'enjeu de la corruption des intelligences artificielles

Un risque à moyen et long termes de la massification des contenus erronés générés grâce à l'IA réside dans la pollution des espaces informationnels, mais également dans le risque de « *pollution et d'auto-dégradation des modèles d'IA* [(1)] ».

● **Les IA génératives fonctionnant à l'aide de données d'entraînement, l'authenticité de ces dernières est fondamentale.** Des données corrompues finissent mécaniquement par corrompre le résultat. Il est donc indispensable de parvenir à préserver ces données ; un défi de taille au vu du degré croissant de pollution numérique. Pourtant, « *s'agissant de l'entraînement des modèles, les fournisseurs de modèles pré-entraînés restent souvent opaques sur les données utilisées, ainsi que sur les potentiels biais dans les réponses des IA génératives* [(2)]. » Des sites avérés de désinformation peuvent ainsi être utilisés comme des sources par des IA car « *pour éviter de fournir des réponses trompeuses, certains services s'appuyant sur des modèles d'IAg proposent des sources pour étayer leur réponse, mais sans analyse préalable de la qualité de l'information de celles-ci. Ainsi, Newsguard* [(3)] *a démontré que certains services d'IAg utilisent comme source pour générer leurs réponses des sites du dispositif pro-russe* Portal Kombat *détecté et caractérisé par VIGINUM*. » En effet, un audit de NewsGuard publié en juin 2024 a révélé que les principaux chatbots d'IA générative occidentaux répétaient des récits de désinformation liés à Storm-1516 dans 32 % des cas, en raison du blanchiment stratégique de ces récits par le biais de faux sites d'information locaux et de vidéos de prétendus lanceurs d'alertes diffusées sur YouTube [(4)] .

● **La corruption algorithmique peut également intervenir dès la conception de l'IA générative.** De sérieux doutes existent ainsi quant à la fiabilité de l'IA générative chinoise *DeepSeek* [(5)]. Selon un rapport de la Chambre des Représentants des États-Unis, le chat bot de *DeepSeek* modifierait ou supprimerait

---

(1) Enjeux systémiques - février 2025 – Défis et opportunités de l'intelligence artificielle dans la lutte contre les manipulations de l'information, Viginum.

(2) Ibid.

(3)Newsguard, « October 2024 -- French-Language AI Misinformation Monitor". (lien).

(4) McKenzie Sadeghi, Newsguard, 18 juin 2024. (lien).

(5) « It has been reported that the DeepSeek chatbot alters or suppresses responses to topics deemed politically sensitive by the CCP in 85 % of cases, directly aligning outputs with Beijing's censorship directives » Rapport du Select Committee on the Chinese Comunist Party, Chambre des représentants des Etats-Unis, 16 avril 2025, p. 5.

les réponses aux sujets considérés sensibles par le parti communiste chinois dans 85 % des cas.

● **« L'empoisonnement » des réponses des chatbots et la manipulation des grands modèles de langage (LLM) d'IA peuvent ainsi relever de stratégies malveillantes délibérées**. Cette situation est d'autant plus préoccupante que les LLM sont utilisés de manière croissante par les citoyens et les entreprises, pour faire des recherches en ligne mais également dans un cadre professionnel. Pourtant, un système de décision qui reposerait en partie sur l'IA s'avérerait ainsi particulièrement vulnérable et prévisible.

2. La création d'une fonction « influence » afin de faire face à l'intensité croissante de la compétition dans le champ des perceptions

Pour faire face à l'accroissement de la compétition dans le champ des perceptions, décrite supra, la création d'une fonction stratégique influence vise à mieux organiser la réponse de l'État.

Si elle permet d'afficher clairement la volonté française de sortir de la naïveté, la nouvelle fonction stratégique repose en revanche sur le concept relativement flou de « l'influence ».

a. La volonté affichée de sortir de la naïveté

● **La consécration d'une nouvelle fonction stratégie « Influence » dans la revue nationale stratégique de 2022 (RNS) témoigne de la volonté française d'assumer le rapport de force dans ce domaine pour préserver ses intérêts nationaux.**

Le discours du Président de la République à Toulon le 9 novembre 2022, qui annonce la création de la fonction stratégique « Influence », témoigne de cette prise de conscience. « *La deuxième grande orientation que nous devons prendre est celle du champ des perceptions, dont l'importance va croissant, et que nous devons investir avec une détermination nettement accrue. (…) Nous ne serons pas les spectateurs patients de cette évolution. Nous devrons savoir la détecter sans délai, l'entraver et à notre tour, -mais à la manière d'une démocratie-, la devancer, en user à notre profit dans les champs numériques et physiques.* » Face à ce constat, le Président de la République dresse des lignes d'action *« Convaincre fait partie clairement des exigences stratégiques, mais nous devons profondément revoir nos voies et moyens de le faire dans ce nouveau contexte. Il nous revient ainsi de penser la promotion, sans orgueil, mais sans inhibition malvenue, de notre cause. Une attitude qui serait seulement réactive, voire défensive, pourrait passer pour une forme de passivité. Ce ne sera pas la nôtre. Aussi l'influence sera-t-elle désormais une fonction stratégique, dotée de moyens substantiels, coordonnée au plan interministériel, avec, pour sa déclinaison internationale, un rôle central du ministère de l'Europe et des Affaires étrangères.* »

● **La RNS de 2022 consacre ainsi l'influence comme une nouvelle fonction stratégique à part entière**, aux côtés des fonctions « connaissance-compréhension-anticipation », « dissuasion », « protection-résilience », « prévention » et « intervention ». Selon les auteurs de la RNS, « *l'agressivité dont font preuve nos compétiteurs nous rappelle en effet que rien n'est acquis : outre nos intérêts diplomatiques, économiques et stratégiques, les nouvelles batailles de l'influence mettent en jeu notre capacité à faire vivre le modèle français et européen et à faire comprendre et accepter l'engagement de la France sur la scène internationale. Il nous faut donc assumer plus directement le rapport de forces dans ce champ pour défendre l'intérêt national.* »

La RNS dégage en outre des principes et lignes directrices devant guider l'action : « *La France doit être capable de contrer et maîtriser les effets de ces agressions hybrides, dans le respect de ses principes et de ses valeurs.* » Pour autant, le document indique que la France ne s'interdit pas d'agir et de développer des outils de riposte contre les sociétés militaires privées, groupes armés ou milices utilisés comme intermédiaires par des puissances hostiles à travers la « *diffusion d'informations, sanctions nationales ou européennes, poursuites judiciaires, voire actions militaires (qui) pourront cibler ces groupes s'ils mènent des activités préjudiciables aux intérêts français ou s'ils sont responsables d'atteintes aux droits humains et de crimes de guerre.* »

b. L'influence : un concept plastique à la définition délicate

Le choix du concept « d'influence » reflète le caractère polymorphe et évolutif des stratégies hybrides visées, qui ne relèvent pas exclusivement du champ informationnel. Ce choix d'un concept plastique, mais néanmoins assez vague, soulève toutefois des enjeux de définition. Ainsi, dans son numéro consacré à l'influence [(1)], les contributeurs de la Revue de défense nationale pointaient un « *brouillard sémantique et conceptuel,* » brouillard qu'il convient de dissiper pour passer à l'action.

● **La notion d'influence est par essence large et peu aisée à définir.** Elle s'inscrit traditionnellement dans une dialectique l'opposant à la notion de puissance mais, force est de constater que l'influence tend parfois à devenir la continuation de la guerre par d'autres moyens. Selon la définition donnée par la RNS de 2022, la fonction stratégique influence « *vise à promouvoir et à défendre les intérêts et les valeurs de la France. Il s'agit d'un volet essentiel à l'expression de puissance*. »

Ne se réduisant ni au lobbying ni à la propagande, notions auxquelles elle est fréquemment associée, l'influence peut se définir comme un moyen qu'un État construit par l'emploi simultané et conjugué de plusieurs outils, afin de créer des alliances ou des communautés d'intérêts, qui porteront d'autres États à agir d'une façon qui ne sera pas opposée à ses intérêts, voire d'une façon qui lui serait

(1) Laurent, S.-Y. (2025). Introduction. L'information(nel) : brouillard sémantique et conceptuel. Revue Défense Nationale, 876(1), 9-10. (lien).

favorable [1]. Ainsi, l'influence désigne la capacité à agir sur les perceptions pour modifier les attitudes et les comportements dans un sens favorable aux intérêts de « l'influenceur » ou défavorable à ceux de ses compétiteurs et adversaires.

L'influence est consubstantielle à la diplomatie. Elle peut être prolongée par des opérations de communication d'influence. En s'adressant aux ambassadeurs le Président de la République l'a défini comme le fait « *d'être bien vu, au maximum aimé, être compris, si possible suivi* [2].»

L'influence est distincte du *soft power*, théorisé par Joseph Nye, qui reflète une attraction plus spontanée et en même temps plus diffuse, car elle peut être travaillée de manière stratégique. Toutefois, elle diffère de la propagande, fondée sur le mensonge et la manipulation.

Enfin, l'influence ne se résume pas entièrement à la communication stratégique ni au concept de « StratCom » d'origine otanienne, bien que la communication puisse constituer un outil. *« Alors qu'une action de communication stratégique suppose qu'un acteur institutionnel identifié délivre un message à un public cible dans le but de modifier ses perceptions, dans le cadre de la lutte informationnelle, l'émetteur s'appuie sur des relais indirects pour diffuser un contenu persuasif qui modifie les perceptions de la cible »* [3]. La notion de « Stratcom », introduite en 2018 dans la doctrine des armées françaises a, par ailleurs, été abandonnée en 2023 au profit de la notion d'influence.

Aussi, **plus que la simple communication stratégique, il ressort des auditions menées par vos rapporteures, que la fonction influence dans son acception large intègre aussi bien la contre-influence et la lutte informationnelle, défensive comme offensive.**

● L'influence diffère de la notion d'ingérence, principalement à travers la finalité recherchée, bien que les deux notions soient parfois imbriquées au sein d'une stratégie d'ensemble.

Si l'influence, fait partie de l'action normale des États pour défendre ouvertement leurs intérêts et les valeurs qu'ils portent, l'ingérence en est la prolongation hostile. Comme l'indiquent les membres de la délégation parlementaire au renseignement (DPR) dans leur rapport annuel d'activité 2022-2023, « *si l'influence d'un État relève d'une stratégie au long cours – un soft power revendiqué et motivé par un désir de rayonnement – l'ingérence renvoie à une action dissimulée et malveillante. Commanditée depuis l'étranger, elle vise à porter atteinte, autrement que par la confrontation militaire, aux intérêts fondamentaux d'un pays et à sa souveraineté dans toutes ses dimensions politiques*,

---

(1) Bertrand DEBRAY. « Quelle contribution militaire à la stratégie d'influence de la France ? », Cahiers de la RDN, Idées de la guerre et guerre des idées - Regards du CHEM - 71e session.

(2) Discours du Président de la République, conférence des Ambassadeurs de 2023. (lien).

(3) Collectif Thot, (2025). Entre « lutte informationnelle » et « guerre cognitive », la souveraineté en question Menaces sur la démocratie et sur le système de décision. Revue Défense Nationale, 876(1), 96-104. (lien).

juridique, militaire, économique et technologique. » Toutefois, « *bien que leurs finalités ne soient pas comparables, il existe néanmoins des porosités entre influence et ingérence, une zone grise voire un continuum en ce sens que l'influence peut aussi préparer le terrain à des actions d'ingérence*. »

L'ingérence revêt ainsi un caractère hostile, secret et répréhensible, là où l'influence consiste dans une démarche visant à orienter une situation en se fondant sur la conviction et la séduction. Toutefois, il existe un *continuum* qui, à partir de l'influence, s'aggrave vers l'ingérence, puis le haut du spectre de l'hybridité (actions cinétiques), et enfin le conflit ouvert.

Selon les informations fournies par le SGDSN à vos rapporteures, par sa portée étendue à toutes les composantes de la société et sa manifestation privilégiée dans le monde numérique et les réseaux sociaux en particulier, **la lutte informationnelle constitue aujourd'hui un des principaux leviers d'ingérence,** avec une capacité désormais avérée à fragiliser les équilibres sur lesquels reposent nos sociétés ouvertes et démocratiques.

B. UNE FONCTION STRATÉGIQUE NECESSAIREMENT INTERMINISTÉRIELLE ET À L'ARCHITECTURE COMPLEXE, MAIS DONT LA STRUCTURATION PROGRESSE

La RNS de 2022 désigne le ministère de l'Europe et des affaires étrangères comme chef de file de la fonction stratégique « Influence » et prévoit qu'une *« organisation plus agile, réactive et mieux intégrée sera adoptée pour identifier, caractériser, déclencher les mécanismes de protection adaptés et élaborer des réponses dans une approche davantage multisectorielle. »*

Un dispositif interministériel a été mis en place selon deux volets : d'une part, un volet défensif assimilable à la lutte contre les opérations d'influence et les manœuvres informationnelles ciblant notamment le territoire national et, d'autre part, un volet plus proactif, voire offensif, d'influence et de lutte informationnelle à destination de l'international.

Bien que l'organisation retenue ait produit de premiers résultats très positifs, vos rapporteures font le constat d'une architecture qui demeure complexe et peu lisible de l'extérieur.

1. Une organisation interministérielle en cours de consolidation

a. Le choix d'une approche interministérielle et multidimensionnelle : une fonction stratégique dont le chef de filât a été confié au ministère de l'Europe et des affaires étrangères

● **Le choix fait dans la RNS de 2022 est celui d'une fonction stratégique « influence » inscrite dans une stratégie multifactorielle de temps long qui dépasse le champ militaire**. En effet, « *l'influence ne se décrète pas, elle se construit* » comme le rappelle Frédéric Charillon, auteur de *Guerres d'influences, Les États à la conquête des esprits* (2022).

En conséquence, le ministère de l'Europe et des affaires étrangères a été désigné comme chef de file interministériel et a été chargé de l'élaboration de la stratégie nationale d'influence. Toujours selon la RNS de 2022, « *cette organisation s'appuie sur une stratégie nationale d'influence qui doit inscrire les actions menées dans une approche globale et sur le temps long pour valoriser les engagements de la France mais aussi pour répondre ou riposter de façon efficace à des manœuvres ou à des attaques informationnelles contre ses intérêts. Elle mobilise sa diplomatie publique, en particulier en Afrique. Une communication stratégique est déclinée afin de porter un message cohérent, crédible et efficace vers les compétiteurs, les partenaires ou alliés et vers l'opinion publique nationale et internationale. Elle peut être coordonnée avec les alliés*. »

À cet égard, la France dispose de nombreux atouts. Comme le rappelle la RNS précitée, la France bénéficie d'un poids politique majeur du fait de son siège de membre permanent du Conseil de sécurité des Nations unies, de son statut d'État doté et de sa présence Outre-mer, d'un modèle complet d'armée et de troupes déployées sur de nombreux continents, de son attractivité économique, de la langue française parlée par 300 millions d'individus, d'une image positive du fait de son influence culturelle, de la projection globale soutenue par l'universalité du réseau diplomatique, culturel et éducatif ou encore de ses partenariats de sécurité.

● La création d'**un dispositif interministériel dédié doit permettre de décliner la fonction stratégique « influence » dans le champ informationnel**.

Si la RNS de 2022 ne mentionne que le terme d'influence, vos rapporteures ont cherché à clarifier l'organisation sous-jacente et à replacer la nouvelle fonction stratégique dans un contexte plus large allant de la lutte contre les manipulations de l'information à la lutte informationnelle.

Ainsi, trois opérateurs principaux – VIGINUM, le Ministère de l'Europe et des affaires étrangères et le Ministère des armées – concourent à la fonction stratégique influence de manière complémentaire, chacun dans leur champ de responsabilité.

Trois domaines en matière informationnelle ont été présentés à vos rapporteures :

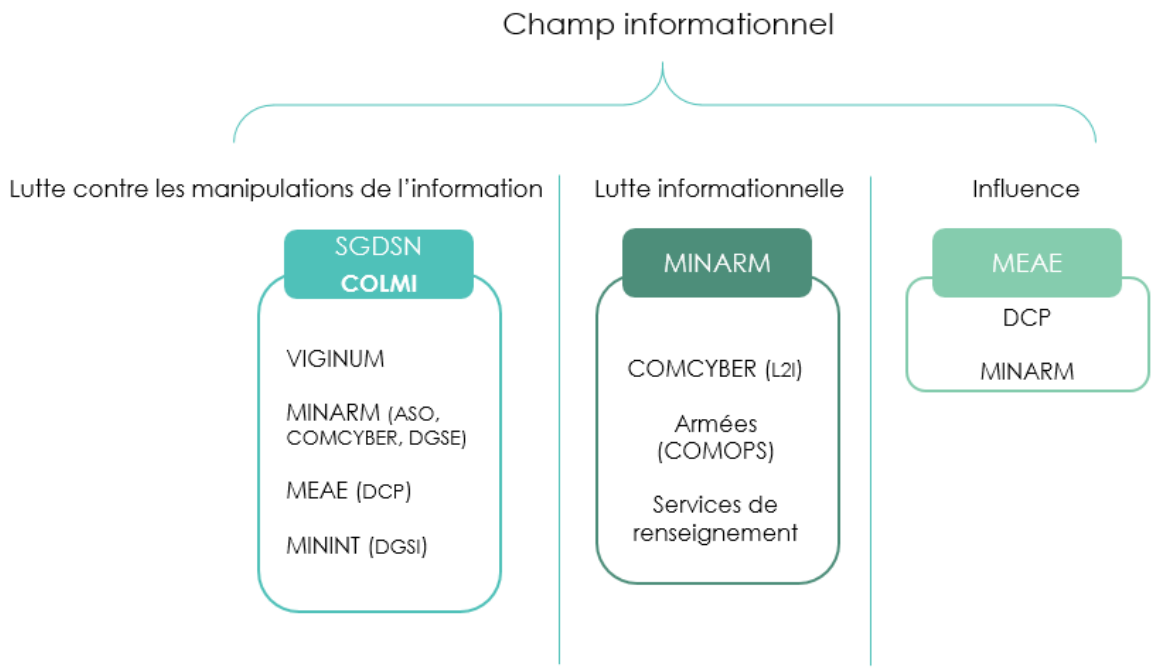
– **La lutte contre les manipulations de l'information** (volet défensif) : constitue une prérogative du Premier ministre et une compétence du SGDSN, qui dispose pour ce faire d'une gouvernance dédiée (le comité opérationnel de lutte contre les manipulations de l'information dit COLMI) et d'un opérateur (VIGINUM). Il s'agit de protéger le débat public numérique français lié aux intérêts fondamentaux de la Nation.

– **La lutte informationnelle** (volet offensif) : Le ministère « menant » est le ministère des armées, appuyé par les services. La mission est autre puisqu'il s'agit d'engager un rapport de force dans le champ informationnel et de combattre l'adversaire lorsque la présence militaire française est attaquée. La mission consiste à agir contre les actions hostiles de compétiteurs, notamment sur les théâtres d'opérations.

– **L'influence au sens strict** (volet proactif, de promotion des intérêts et des valeurs françaises) : prérogative du ministère de l'Europe et des affaires étrangères, qui s'adresse aux audiences internationales. Proactive, cette fonction vise à défendre l'image de la France à l'étranger, promouvoir une image positive et façonner un environnement international favorable aux intérêts français. L'outil principal utilisé est la communication stratégique et la diplomatie publique.

Toutefois, ces trois domaines de lutte se recoupent pour partie. Par exemple, le ministère de l'Europe et des affaires étrangères et le ministère des armées participent également à la lutte contre les manipulations de l'information lorsque qu'un ministre dénonce publiquement une ingérence étrangère. Aussi, **chaque opérateur précité agit-il davantage comme un « coordonnateur » ou un « chef de file » du domaine de lutte.**

DOMAINES EN MATIÈRE INFORMATIONNELLE ET MINISTÈRES CHEF DE FILE



Source : schéma réalisé par la mission d'information sur la base des auditions menées

● Par ailleurs, au sein de ces domaines, trois missions principales peuvent être distinguées : **l'analyse, la riposte et la réponse proactive,** appelée aussi communication stratégique et d'influence.

Au sein du ministère de l'Europe et des affaires étrangères, il convient de mettre en avant le rôle de la sous-direction veille et stratégie (VS) de la direction de la communication et de la presse (DCP), qui connaît une transformation d'ampleur pour répondre aux enjeux de la nouvelle fonction stratégique. La direction de la communication et de la presse, intervient plus particulièrement en ce qui concerne les enjeux d'influence dans le champ informationnel (presse, communication institutionnelle renouvelée, réseaux sociaux, etc). En son sein, la sous-direction de la veille et de la stratégie, est active depuis novembre 2022. Selon les informations fournies par le ministère de l'Europe et des affaires étrangères à vos rapporteures, son mandat porte sur la modernisation de l'analyse du champ informationnel, la riposte face aux manipulations de l'information, la communication stratégique et d'influence et le développement de partenariats interministériels et internationaux (SEAE, OTAN, G7, OCDE), comme avec la société civile (ONG, organismes de recherche). La sous-direction a été formée via le redéploiement de 11 agents et de 14 recrutements depuis 2023, et réunit actuellement 24 agents répartis en trois pôles (analyse médias ; analyse réseau sociaux ; communication stratégique). 9 postes ont été créés en 2023, 5 en 2024.

Tout d'abord, le volet analytique a été modernisé (i).

Selon les informations fournies par le ministère de l'Europe et des affaires étrangères, la fonction « alerte/analyse » a été entièrement modernisée. Le ministère livre aux autorités presque en temps réel la « température » sur les réseaux sociaux et les écosystèmes médiatiques dans toutes les zones prioritaires grâce à la réorganisation des remontées d'informations par les postes. Le ministère indique développer et optimiser ses outils dans un environnement juridique et financier très contraint.

Toutefois, le ministère de l'Europe et des affaires étrangères n'est pas le seul à assurer cette fonction. En interministériel, des complémentarités ont été développées entre la veille de la DCP, celle du COMCYBER et celle de VIGINUM. Le SGDSN, chargé avec VIGINUM de coordonner les détections et les caractérisations des ingérences numériques étrangères qui visent la France, est avant tout concerné par les campagnes inauthentiques de manipulation de l'information visant les intérêts fondamentaux de la Nation. La contribution du ministère de l'Europe et des affaires étrangères est pilotée par la sous-direction VS qui a développé une veille analytique jugée complémentaire, en s'appuyant sur les remontées du réseau diplomatique, ce qui doit permettre à la France de détecter, bien en amont, des signaux faibles. VS développe en outre une méthodologie pour analyser les dynamiques de rebond entre les ingérences numériques, la communication officielle et le traitement médiatique grand public. Cette analyse dite à 360° (audiovisuel, presse, réseaux sociaux) qu'offre le ministère à l'effort interministériel permet de dégager les tendances à l'œuvre selon les zones géographiques.

Ensuite, le volet défensif repose sur une riposte opérationnelle de mieux en mieux coordonnée (ii).

La réponse de l'État peut être d'ordre politique (dénonciation publique, déclaration politique d'attribution, publication d'un rapport technique), ou diplomatique avec notamment des propositions de gels des avoirs et de sanctions au niveau de l'Union européenne (UE), lorsque les individus ou personnes morales concernés entrent dans le champ de ces régimes.

Christophe Lemoine, directeur de la communication et de la presse du ministère de l'Europe et des affaires étrangères, auditionné par vos rapporteures, estime qu'une première étape dans la réponse a été franchie en matière de riposte et de lutte contre les manipulations de l'information, qu'il juge désormais pleinement intégrées dans le métier diplomatique et l'action des ambassades. Des campagnes d'acteurs agressifs, comme la Russie, ont ainsi fait l'objet de plusieurs dénonciations publiques, en lien avec VIGINUM.

Enfin, le volet proactif s'inscrit dans le cadre de la communication stratégique de la France à l'étranger (iii).

Le ministère de l'Europe et des affaires étrangères indique avoir mené en 2023 et en 2024 des campagnes de communication partout dans le monde sur les échecs russes en Ukraine et avoir appuyé les Ukrainiens dans leur plaidoyer. Par exemple, la France a fait adopter en juillet 2023 des sanctions européennes contre des opérateurs de désinformation comme la *Social Design Agency* pour leur implication dans la campagne de désinformation *Doppelgänger*. Ces sanctions ont ensuite été reprises par les États-Unis et le Royaume-Uni. De nouvelles sanctions ont également été obtenues en décembre 2024.

La DCP estime que le dispositif, pourtant récent, a pu faire ses preuves. Ainsi, pendant les Jeux olympiques et paralympiques (JOP) 2024, selon le Quai d'Orsay, la coordination interministérielle mise en place a permis un repérage des manœuvres par VIGINUM, puis des dénonciations publiques en amont des JOP par le Quai d'Orsay devant la presse.

● L'ensemble des services du ministère de l'Europe et des affaires étrangères, du réseau diplomatique et de ses opérateurs contribuent par ailleurs à la fonction influence à différents titres.

Selon les informations fournies par le ministère de l'Europe et des affaires étrangères, la France assure une présence plus active et systématique dans les institutions multilatérales, dans le débat d'idées (à travers le centre d'analyse, de prévision et de stratégie (CAPS), par exemple, qui noue des partenariats avec de nombreux forums ou think tanks) et les lieux prescripteurs de la conversation internationale, terrains privilégiés de la compétition des modèles et de la contestation des normes, en y soutenant notamment la présence française et européenne dans les postes de direction et d'experts. Selon les informations fournies à vos rapporteures, la création du Forum de Paris sur la Paix visait par exemple à renforcer la place de Paris comme lieu prescripteur.

Elle agit également par sa diplomatie culturelle, une coopération technique dans tous les domaines, civil et militaire, étatique ou décentralisée, une diplomatie sportive, l'éducation – *au sein, notamment, des 580 établissements scolaires à l'étranger, qui scolarisent quelque 400 000 élèves, dont 70 % d'élèves étrangers, en forte croissance* – par l'accueil de 400 000 étudiants étrangers, ainsi que, sous la bannière de la « stratégie Talent », de chercheurs, intellectuels et artistes étrangers. Elle agit aussi par sa diplomatie économique et une politique d'attractivité du territoire national à l'adresse des entrepreneurs et investisseurs étrangers, ainsi que par la promotion de Paris comme principale place boursière de la zone euro et premier centre financier de l'Union européenne. Elle agit, enfin, par ses nombreuses initiatives relatives aux enjeux globaux, qu'il s'agisse du climat, de l'environnement, de la santé, du numérique et de l'intelligence artificielle ou de la réforme du système financier international. Selon la DCP, ces actions, que le renforcement des moyens engagé à la suite des « états généraux de la diplomatie »

a permis de faire monter en puissance, sont partie intégrantes de l'image et, partant, de l'influence française.

En revanche, alors que les pays africains, notamment du Sahel constituent une zone d'effort pour l'influence française, vos rapporteures relèvent avec interrogation le fait que le poste d'Ambassadeur thématique pour la diplomatie publique en Afrique n'ait pas été renouvelé.

b. La dichotomie entre l'influence (à destination de l'international) et la lutte contre les manipulations de l'information (sur le territoire national)

● La réponse interministérielle, telle qu'elle existe aujourd'hui, repose sur une séparation entre l'influence (à destination de l'international) et la lutte contre les manipulations de l'information (essentiellement sur le territoire national).

Selon vos rapporteures, ces deux versants de la fonction stratégique « Influence » ne peuvent être considérés isolément et s'apparentent davantage à un *continuum*. Les deux politiques publiques reflètent en réalité pour partie les volets « défensif » et « offensif » de la réponse étatique aux manipulations de l'information et aux stratégies d'influence malveillantes. Aussi, les personnes auditionnées ont-elles insisté sur le fait que les actions d'influence ne s'adressaient pas à l'opinion publique nationale, mais s'exerçaient uniquement en dehors des frontières françaises.

Si vos rapporteures ont été sensibilisées au fait que la séparation entre les volets défensif et offensif constituait une garantie importante pour la démocratie, elles relèvent néanmoins que cette distinction ne saurait être absolue puisque l'espace informationnel étant par nature ouvert et mondialisé, une action d'influence menée à l'étranger peut avoir des répercussions sur l'opinion publique nationale.

● Dans ce cadre, VIGINUM constitue l'opérateur de référence pour la protection du débat public numérique français, même si sa création précède d'un an la consécration de la fonction Influence par la RNS.

En effet, la création du « service de vigilance et de protection contre les ingérences numériques étrangères », rattaché au SGDSN, sur décision du Président de la République en 2021, vient pallier un manque dans le dispositif de protection de la sphère informationnelle française. VIGINUM est ainsi née du constat que l'État n'avait pas la capacité de se défendre en matière de lutte contre les manipulations de l'information et en particulier contre une opération d'ingérence numérique étrangère d'ampleur. Selon les personnes auditionnées par vos rapporteures, le déclencheur semble avoir été triple : l'avènement des *Macron Leaks* durant la campagne présidentielle de 2017 ; la virulence de la campagne informationnelle antifrançaise consécutive au discours du Président de la République après l'assassinat terroriste de Samuel Paty et, plus récemment, les campagnes informationnelles agressives contre les intérêts français au Sahel.

Avant sa création en 2021, une structure de coordination existait déjà en interministériel à travers le CLMI mis en place concomitamment à l'adoption de la loi de 2018 contre la manipulation de l'information [(1)]. Pour faire face à la vague importante de désinformation en matière de santé pendant la crise de la covid-19, il a ensuite été décidé de créer une cellule de crise dédiée au SGDSN, baptisée « la *task force* Honfleur », sorte de préfiguration qui précède la création de VIGINUM.

Le champ de compétence de VIGINUM est strictement encadré par deux décrets. Au titre des attributions qui lui sont confiées par l'article 3 du décret n° 2021-922 du 13 juillet 2021, VIGINUM a pour missions de **détecter et de caractériser les opérations d'ingérences numériques étrangères (INE) en analysant les contenus publiquement accessibles sur les plateformes en ligne.** Pour ce faire, VIGINUM est autorisé par le décret n° 2021-1587 du 7 décembre 2021 à opérer un traitement automatisé de données à caractère personnel.

Volet numérique de la manipulation de l'information, **l'ingérence numérique étrangère** se définit comme une opération « *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* ».

c. Une organisation à clarifier

À l'issue de leurs travaux vos rapporteures font le constat d'une architecture complexe, concernant un grand nombre d'acteurs, qui possèdent chacun une compétence partielle en matière d'influence ou de lutte contre les manipulations de l'information, malgré l'existence d'efforts réels de coordination en interministériel.

i. Une architecture complexe

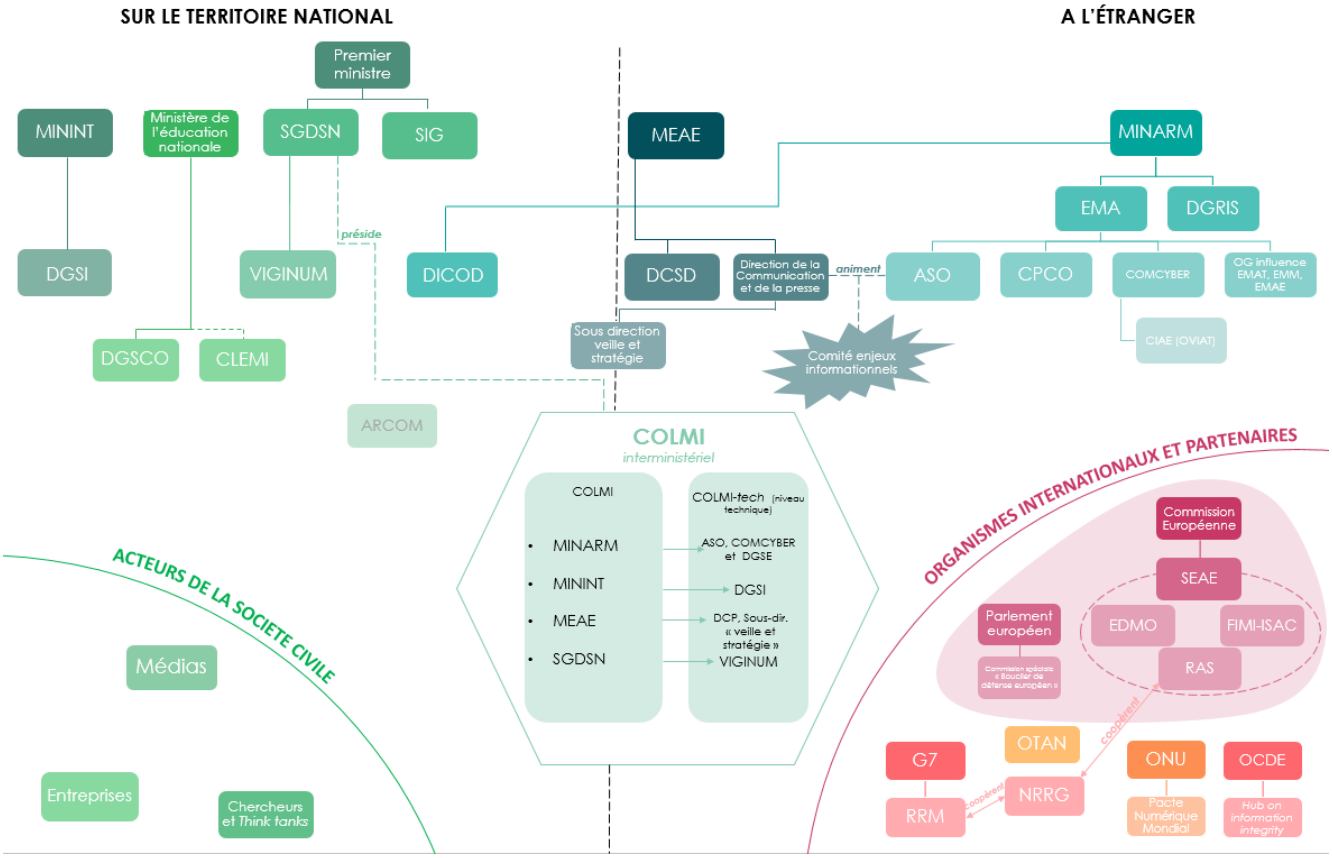
Le constat d'un manque de lisibilité du dispositif est partagé par les auteurs du rapport d'enquête sénatorial portant sur les ingérences étrangères [(2)], qui relevaient notamment un « dispositif de protection étoffé mais à géométrie variable, sans stratégie d'ensemble », pointant le risque d'une « archipelisation » des capacités et de dispersion des moyens de réponse, assortie de l'absence d'une doctrine claire de riposte aux manœuvres hostiles.

---

(1) LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

(2) Rachid Temal, Rapport de la commission d'enquête sur les politiques publiques face aux opérations d'influences étrangères, Sénat (juillet 2024).

CARTOGRAPHIE DES ACTEURS DE L'INFLUENCE ET DE LA LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION



Source : Schéma réalisé par la mission d'information

ii. Une coordination interministérielle qui s'effectue essentiellement *via* des comités spécialisés dédiés : le comité opérationnel de lutte contre les manipulations de l'information (COLMI) et le comité « enjeux informationnels »

Si à l'origine le ministère de l'Europe et des affaires étrangères était absent de la comitologie, la coordination interministérielle a sensiblement progressé depuis 2022. Selon les informations fournies à vos rapporteures, la gouvernance de la fonction Influence repose actuellement principalement sur **deux comités interministériels de coordination spécialisés.**

● S'agissant du **volet défensif,** l'ensemble des acteurs concernés est rassemblé au sein du **comité opérationnel de lutte contre les manipulations de l'information (COLMI)**, présidé par le SGDSN et animé par VIGINUM.

Le COLMI constitue une enceinte permettant de partager la connaissance sur la menace informationnelle à fin d'imputation et développer des stratégies de réponse à ces menaces. C'est dans cette enceinte que sont notamment coordonnées les séquences de dénonciation publique de campagnes numériques de manipulations de l'information, sur le fondement des fiches techniques ou des rapports publics publiés par VIGINUM.

Au niveau stratégique le COLMI réunit notamment une fois par mois le comité de veille et de stratégie du ministère de l'Europe des affaires étrangères (MEAE), les services du ministère des armées (MINARM), dont la DGSE, et le ministère de l'Intérieur (DGSI).

Par ailleurs, le « COLMI Tech », se réunit une fois par semaine et rassemble surtout des techniciens opérationnels, pour dresser notamment un état de la menace.

● S'agissant du volet **proactif, voire offensif**, les actions semblent se coordonner autour d'un **« comité enjeux informationnels »,** qui succède à la *task force* interministérielle informationnelle (TF2I) et réunit notamment le MEAE, le MINARM, l'état-major particulier du Président de la République et les services. Un autre comité exécute et traduit le cas échéant les objectifs arrêtés en campagnes.

● Selon les personnes auditionnées, la recherche de l'efficacité de la coordination interministérielle doit être poursuivie et suppose des efforts continus pour surmonter l'écueil du travail en silos.

La comitologie née ces deux dernières années semble permettre aujourd'hui une coordination interministérielle efficace dans le domaine de la détection et du partage de l'information. Dans le dernier numéro de la RDN paru en janvier 2025, le général de corps d'armée Bonnemaison, COMCYBER, réaffirmait néanmoins la nécessité d'une double coordination horizontale et verticale « *À cette intégration horizontale des trois domaines de lutte informatiques dans le combat classique s'ajoute aussi nécessairement une coordination verticale avec la nouvelle fonction stratégique « influence », dans son approche militaire puis interministérielle.* »

Le fonctionnement en interministériel doit en effet permettre de détecter au plus tôt les attaques, en identifiant les signaux faibles dans la sphère informationnelle et en prenant rapidement les mesures nécessaires pour rétablir les faits, caractériser l'attaque et, le cas échéant, dénoncer l'action des compétiteurs ayant initié l'attaque.

2. La structuration progressive d'une fonction « influence et lutte informationnelle » au sein des armées

● Puisque l'information tend à être considérée comme une arme de guerre, avec des opérations qui visent directement les opérations militaires françaises, les armées contribuent directement à la nouvelle fonction stratégique influence, en coordination avec le MEAE, qui en assure le pilotage.

En effet, selon le CEMA, l'action dans le champ des perceptions est un enjeu majeur de crédibilité et d'efficacité opérationnelle. « *Refuser d'y combattre, ou n'y être que passif, rendrait une armée extrêmement vulnérable aux composantes informationnelles des stratégies hybrides et pourrait lui faire « perdre la guerre, avant la guerre ». Par exemple, sa légitimité pourrait être remise en cause avant même un déploiement en influençant négativement sa propre opinion publique, les populations autochtones ou encore des organisations internationales. Par ailleurs,*

en ne s'impliquant pas totalement dans la connaissance des champs immatériels, le risque est grand de subir les désinformations et les intoxications préjudiciables à l'analyse du renseignement, comme à la mesure objective des performances. Les militaires eux-mêmes pourraient également subir les effets directs de manœuvre d'intimidation – par exemple en instrumentalisant les familles –, ou de démoralisation. » [(1)]

● **Le recours aux stratégies indirectes et à l'influence n'est pas un fait nouveau pour les armées, l'influence s'inscrit d'ailleurs pleinement dans la vision du chef d'État-major des armées consistant à « gagner la guerre avant la guerre ».** Dans un contexte militaire, l'influence vise à façonner l'environnement informationnel pour atteindre des objectifs stratégiques. Les armées définissent l'influence comme : « *la capacité à agir sur les perceptions pour in fine modifier les attitudes et les comportements dans un sens favorable à nos intérêts* [(2)] ». La lutte informationnelle (LI) participe directement aux actions d'influence, mais n'en représente qu'une partie. Elle vise principalement à prendre et à conserver l'ascendant dans le champ informationnel face à un ou plusieurs adversaires désignés, afin de produire un ou plusieurs effets préalablement identifiés et validés. Il convient de noter à nouveau que l'influence militaire ne s'exerce qu'à l'extérieur du territoire national dans un cadre strict, respectueux du droit international.

L'influence militaire « *rassemble les capacités militaires dites non-cinétiques d'action sur les perceptions et de modification des comportements. La doctrine militaire française y intègre classiquement les opérations psychologiques, les opérations d'informations, les actions civilo-militaires et une déclinaison dans l'environnement informatique via la lutte informatique d'influence (L2I)* [(3)] . » Pour les armées, l'audience prioritaire des actions d'influence est constituée par les populations étrangères, dans l'objectif de favoriser l'acceptation de la force. Ainsi, des actions civilo-militaires (radio communautaire, réfection de ponts ou d'écoles, distribution de fournitures scolaires) ont-elles également été développées en appui de la manœuvre globale. [(4)]

● Si la prise de conscience des armées est ancienne et antérieure à la RNS de 2022, l'enjeu semble désormais de « passer à l'action, » pour paraphraser la RDN [(5)], voire à l'échelle, pour être en mesure de produire des effets décisifs sur le champ de bataille et acquérir un avantage informationnel, même limité et ponctuel.

---

(1) Burkhard, T. (2023). Pas de stratégie sans influence, pas d'influence sans stratégie. Revue Défense Nationale, 856(1), 9-15. (lien).

(2) CICDE, doctrine interarmées 10 – Influence et lutte informationnelle, 2023.

(3) Nicolas Zubinski. L'influence militaire dans la nouvelle pensée stratégique française. RDN (2021/n° 837).

(4) Burkhard, T. (2023). Pas de stratégie sans influence, pas d'influence sans stratégie. Revue Défense Nationale, 856(1), 9-15. (lien).

(5) L'informationnel : dissiper le brouillard et passer à l'action, RDN, janvier 2025.

a. La prise de conscience anticipée des armées : de la lutte informatique d'influence à la fonction « influence et lutte informationnelle »

Ériger l'influence en fonction stratégique a permis une prise de conscience plus large des enjeux d'influence au sein des différentes armées et au-delà du COMCYBER, déjà responsable de la lutte informatique d'influence.

i. La lutte informatique d'influence

● **Le ministère des armées a joué un rôle précurseur dans la lutte contre les opérations d'influence visant les armées et les intérêts français à l'étranger dans le champ cyber et informationnel.** Dans un contexte de lutte antiterroriste, marqué par la propagande de Daesh, un troisième domaine de lutte a ainsi été confié au COMCYBER : **la lutte informatique d'influence** (L2I), aux côtés de la lutte informatique défensive (LID) et offensive (LIO).

Selon la définition donnée par le COMCYBER, la lutte informatique d'influence (L2I) désigne les opérations militaires conduites dans la couche informationnelle du cyberespace pour détecter, caractériser et contrer les attaques, de façon autonome ou en combinaison avec d'autres opérations. Le périmètre de responsabilité du COMCYBER dans le cadre de la L2I est celui de la protection informationnelle active des forces militaires déployées en opérations hors du territoire national, par anticipation et en riposte.

● **Les opérations de L2I contribuent aux opérations d'influence et de lutte informationnelle des armées.** Elles consistent, pour l'essentiel, à détecter les attaques informationnelles susceptibles de nuire à la réputation des armées ou d'entraver leur action, à les caractériser, à les contrer et à promouvoir l'action des forces. La L2I peut également offrir des opportunités de recueil de renseignement et d'emploi de la ruse.

Comme le précise le général de corps d'armée Bonnemaison, COMCYBER, l'objectif recherché est bien de détecter les attaques informationnelles dans le cyberespace. Il ne s'agit pas de repérer l'avis d'une personne qui serait hostile aux armées, mais bien de détecter des campagnes construites, inauthentiques et coordonnées par un adversaire extérieur qui cherche à nous fragiliser (1). La caractérisation vient ensuite, car « *une opinion personnelle qui nous est hostile n'est pas nécessairement une attaque informationnelle. Pour qu'elle le soit, elle doit être inauthentique, coordonnée et doit utiliser des systèmes d'amplification, comme des fermes à trolls par exemple* (2). »

● **Si la L2I participe de la fonction influence et lutte informationnelle (ILI) dans le cyberespace, elle ne constitue néanmoins qu'un levier parmi d'autres des actions menées par les armées en déclinaison de la nouvelle fonction stratégique influence.**

---

(1)Général Bonnemaison, « combattre dans le cyberespace », site du ministère des Armées. (lien).

(2) Esprit de défense, p.33.

ii. La doctrine ILI, déclinaison militaire de la fonction stratégique « influence »

● **L'aptitude interarmées « influence militaire », dont le périmètre était devenu trop restreint, a été remplacée par l'aptitude « Influence et lutte informationnelle » (ILI) en 2023.** Les armées ont ainsi progressivement structuré une chaine « influence et lutte informationnelle » allant de la veille à la riposte, en passant par des opérations de signalement stratégique, mais également une diversification des offres de coopérations vis-à-vis des partenaires.

● **En effet, les opérations militaires peuvent être des vecteurs d'influence de la même manière que les actions de communication d'influence peuvent appuyer les opérations.** 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* » ; « *la conquête, puis la maîtrise de la supériorité dans le champ informationnel, sont devenues des conditions de la supériorité opérationnelle.* » (1) Ainsi, il ressort des auditions menées par vos rapporteures qu'une stratégie militaire n'intégrant pas l'influence est condamnée à subir celle de l'adversaire.

● **Au sein de la doctrine « ILI », l'on peut distinguer les actions d'influence et de lutte informationnelle, même si les deux composantes se nourrissent l'une de l'autre.**

D'une part, s'agissant de l'influence, les actions s'inscrivent généralement dans le temps long et visent à produire des effets dans le champ des perceptions. Elles n'induisent pas systématiquement une confrontation directe avec un adversaire ou un compétiteur, mais reposent toujours sur la combinaison des actions et des champs matériels et immatériels.

D'autre part, s'agissant de la lutte informationnelle, elle participe directement aux actions et manœuvres d'influence mais n'en représente qu'une partie. Elle vise principalement à prendre et conserver l'ascendant dans le champ informationnel face à un ou plusieurs adversaires désignés. Elle peut être défensive ou offensive, face à un adversaire étatique, paraétatique ou privé.

b. Intégrer nativement l'influence aux opérations militaires

● **Le ministère des armées s'est structuré pour mettre en œuvre la nouvelle fonction stratégique et cherche à renforcer l'intégration native de l'influence sans ses opérations.**

● **Il existe cependant un véritable enjeu d'opérationnalisation de cette nouvelle fonction** (création d'une organisation *ad hoc*, intégration native dans les

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

opérations, synchronisation des effets, extension aux différents niveaux : stratégiques, opératifs et tactiques) et de bonne articulation en interne, notamment avec la communication stratégique.

i. Le rôle central de la cellule ASO, gardienne de la cohérence d'ensemble et pilote de la déclinaison opérationnelle de la fonction ILI

● **La cellule Anticipation stratégique et orientations (ASO) de l'État-major des armées est la tête de chaîne au sein des armées pour la fonction influence et lutte informationnelle.** Créée en 2022 et constituée d'une dizaine de personnes, la cellule ASO joue un rôle de cadrage stratégique et de coordination de la communauté ILI du ministère des armées, qui rassemble de nombreuses parties prenantes : relations internationales militaires, communicants institutionnels et opérationnels, COMCYBER au titre de la L2I, acteurs de la chaine de commandement et de conduite des opérations.

Le pôle ASO réalise trois types d'actions principales :

– assurer la cohérence de l'action militaire en lien avec « l'extérieur » (interministériel et international) ;

– animer et piloter la prise en compte du domaine influence et du champ informationnel des opérations ;

– structurer cette nouvelle fonction selon l'approche « DORESE » (doctrine, organisation, ressources humaines, équipement, soutien et entraînement).

● **La cellule s'assure notamment de la bonne prise en compte de l'influence dans les opérations.** Les questions d'influence et de lutte informationnelle sont intégrées dès la conception d'une opération, qu'il s'agisse de se protéger ou d'amplifier l'action des armées.

Les déploiements des forces intègrent à présent systématiquement le risque informationnel dans l'analyse de risque, afin d'être prêts à réagir en cas de campagne de désinformation visant un déploiement ou encore à communiquer de manière proactive. Aussi, chaque ordre d'opération comporte-t-il dorénavant une annexe influence et lutte informationnelle. « *Plus aucun convoi logistique ne part sans que soit étudié son risque informationnel* », illustre le général de division Jean-Michel Meunier, chef de la cellule ASO, en faisant écho au convoi bloqué au Burkina Faso et au Niger en 2021. « *Nous réfléchissons alors à l'interprétation de nos actions par la population, nous analysons si le terrain informationnel est miné et nous prévoyons des moyens de preuve, comme des capteurs d'images, qui pourraient servir à dénoncer les fausses informations* [(1)]. »

(1) Esprit de défense, p. 33.

L'affaire de Gossi, lorsque l'armée française quitte le Mali en mai 2022, a été un élément déclencheur important pour les armées. Le succès de la manœuvre réalisée repose sur une détection en amont, qui permet de ne pas subir le rythme des adversaires et de prendre l'initiative. Dans ce cas précis, une opération logistique de repli de l'opération Barkhane est planifiée et il ne fait aucun doute qu'elle va se dérouler sous la pression informationnelle de la junte et des mercenaires russes de Wagner. Il est donc décidé de surveiller les bases que l'armée vient de quitter. Les mercenaires de Wagner utilisent les corps de civils qu'ils viennent d'assassiner, et malgré les images et enregistrements audio que la France met en exergue pour contrer le narratif de Wagner, les audiences captives ne sont pas convaincues. La détection précoce d'une manœuvre informationnelle russe permet néanmoins aux armées d'obtenir des images, prises par un drone, montrant des mercenaires du Wagner en train de préparer un charnier sur la base de Gossi, récemment rendue aux forces armées maliennes par la France, afin de l'accuser d'avoir commis un massacre.

Déjouer une campagne avant sa mise en œuvre, lorsque c'est possible, est donc l'option la plus efficace. C'est la raison pour laquelle les armées mènent également des actions de réfutation par anticipation dans le champ informationnel ou *prebunk.* Ainsi, en 2023 un navire de la Marine nationale devait accoster dans le port d'un pays africain tandis que des rumeurs circulaient sur des motivations de l'équipage – des légionnaires suspectés de vouloir envahir le pays ; les armées ont proposé à des influenceurs locaux à forte audience de monter à bord pour réaliser la traversée avec elles et témoigner de leur vie à bord sur les réseaux sociaux. Les fausses informations se sont finalement dissipées et aucune manifestation n'a eu lieu [(1)].

● Pour mettre en œuvre la fonction ILI, **les armées s'appuient sur les chaînes et les commandements déjà existants :** états-majors d'armée chargés d'équiper et de préparer les hommes, chaînes des opérations, commandements spécifiques (COMCYBER, DRM, COM). Les orientations stratégiques sont ensuite déclinées à chaque niveau de commandement (opératif et tactique) qui va porter, dans son périmètre, les effets atteignables par ses capacités. C'est la combinaison de tous ces effets et la cohérence d'ensemble qui constituent les vrais facteurs de succès d'une opération d'influence.

Pour décliner la fonction « ILI » dans chaque armée, l'échelon stratégique s'appuie sur les « officiers généraux influence », qui exercent bien souvent également le rôle de sous-chef opération et activité. Ces officiers généraux sont notamment chargés de conseiller le CPCO pour les actions d'influence en lien avec leur milieu, coordonner l'action des principaux effecteurs et veiller à la bonne anticipation des manœuvres d'influence pour que chaque unité dispose des moyens nécessaires pour contribuer aux opérations d'influence.

(1) Ibid.

● Si les caractéristiques propres de chaque armée constituent autant d'atouts à exploiter pour les opérations d'influence, il ressort des auditions de vos rapporteures que l'armée de Terre semble particulièrement avancée dans la mise en œuvre de la nouvelle fonction stratégique.

S'agissant de la Marine nationale, le milieu dans lequel se déploient les unités se révèle particulièrement propice aux actions d'influence. Les unités sont en effet déployées en dehors du territoire national, aussi bien en haute mer qu'en escale à l'étranger. L'espace aéromaritime favorise le contact entre compétiteurs ; qu'il s'agisse de la méditerranée orientale, ou de la mer Baltique. Selon les personnes auditionnées par vos rapporteures, cette proximité est propice aux prises d'images et à la promotion de narratifs. Les activités en mer Baltique sont par exemple fortement exploitées en terme d'influence. Dans le même temps, il s'agit d'un milieu opaque ; sous la mer pour les forces sous-marines, mais également pour les unités de surface compte tenu des élongations. Selon les informations fournies par l'EMM à vos rapporteures, le *fact-checking* en mer est ainsi très difficile et les compétiteurs en profitent souvent pour avancer un volume de forces déployé très éloigné de la réalité.

De la même manière, le volet influence est consubstantiel aux activités aériennes, par nature très visibles. L'armée de l'air et de l'espace a adapté à la marge son organisation. En exercice ou en opération, les missions d'ILI sont ainsi confiées à une chaîne d'aviateurs dédiés, distincts de ceux en charge de la communication et encadrés par une directive opérationnelle émanant de l'état-major des armées et du CPCO pour ce qui concerne les opérations.

Enfin, la temporalité des opérations aéronavales semble propice au développement d'actions d'influence. Par exemple, la projection du Groupe aéronaval (GAN), de décembre à avril 2025, intégrait nativement un volet informationnel de protection et d'amplification. Selon les informations fournies à vos rapporteures, à chaque escale étaient invités des influenceurs locaux et mises en place des activités de rayonnement. Selon les informations fournies par la Marine nationale, le déploiement du GAN a constitué une réussite : « *se déployer aussi loin, aussi longtemps, avec autant d'interactions, est unique.* » La planification du déploiement et des opérations d'influence qui l'accompagnaient ont été conçues un an à l'avance, à l'image d'une manœuvre militaire à part entière, en définissant des objectifs à atteindre à l'égard des compétiteurs et des alliés.

L'armée de Terre fournit néanmoins à ce jour la composante la plus importante de la capacité influence des armées, appuyée par un organisme spécialisé à vocation interarmées dont la tutelle organique est confiée à l'armée de Terre : le Centre interarmées des actions sur l'environnement (CIAE) crée en 2012 et situé à Lyon.

LES MISSIONS DU CIAE

Le CIAE est un organisme a vocation interarmées à dominante Terre. Il est le centre d'excellence de l'ILI. Ses missions couvrent l'instruction spécialisée et l'appui aux opérations sous différentes formes, notamment la veille, l'analyse, et la production numérique.

Il joue un rôle de contributeur majeur à la notion de « culture française de l'influence », notamment au travers de ses volets formation et incubateur de l'évolution des connaissances et pratiques de l'influence dans le registre militaire.

Il possède une composante actions numériques placée sous le contrôle opérationnel du COMCYBER. Le CIAE comprend les effecteurs L2I qui conduisent des opérations d'influence dans le cyberespace, dans le cadrage opérationnel défini par le COMCYBER.

Depuis 2023, l'armée de Terre a mis en place un dispositif d'organisation de la cohérence du message et de coordination des actions de la composante Terre en appui des opérations. Il se réunit toutes les semaines pour travailler à la convergence des effets informationnels réalisés par l'armée de Terre. L'armée de Terre a également lancé un grand chantier RH pour prendre en compte les dimensions « formation » et « essor du vivier » existant. L'armée de Terre investit près de 300 postes inscrits dans la loi de programmation militaire (LPM) 24-30 et développe son schéma capacitaire propre, complémentaire aux travaux menés en parallèle pour la description d'un schéma directeur interarmées.

À titre d'exemple, **l'armée de Terre est entrée dans un processus de création d'unités d'action d'influence.** Selon les informations fournies à vos rapporteures, les capacités en construction sont toutes tournées vers les opérations et doivent faciliter de manière concrète l'intégration du champ informationnel dans le combat multi-milieux multi-champs (M2MC), qui constitue aujourd'hui le référentiel des opérations. Elles déclinent des capacités qui doivent permettre de réaliser des actions de lutte informationnelle (bataille des narratifs et lutte contre la désinformation) et de mener des opérations de déception pour réduire la transparence du champ de bataille et prendre l'avantage sur l'ennemi en situation de haute intensité.

Parmi les activités menées par les armées, l'on peut notamment citer :

– L'appui et le relais des messages de l'EMA, au travers des *VIP Days*, de la communication opérationnelle, des voyages de presse en présence de la presse internationale, ou bien de la diffusion de contenu sur les réseaux sociaux vers des audiences internationales (en anglais).

– Les opérations de signalement stratégique, qui visent à montrer aux compétiteurs et aux alliés la crédibilité opérationnelle des armées françaises, se distinguent par leur caractère extraordinaire, « envoyant un signal » par leur temporalité, leur ampleur, leur nature, ou bien le message porté, à l'image de la projection du bataillon français en mars 2022 en Roumanie en 30 jours, réaffirmant la volonté française de se positionner en tant que Nation-cadre au sein de l'Alliance

atlantique. L'exercice PIKNE en Estonie-Finlande en décembre 2024 en est un autre exemple.

– Les engagements physiques de long terme qui manifestent la crédibilité de la France et rassurent ses alliés : les missions opérationnelles AIGLE en Roumanie et LYNX dans les pays baltes, par exemple.

– Les actions de partenariat militaire opérationnel (PMO) permettent enfin de faire monter en compétence les armées partenaires et de maintenir des liens, notamment en Afrique où l'image des armées a été durablement entachée sous les effets des campagnes de désinformation de compétiteurs.

● **Toutefois, la création d'une capacité opérationnelle prend du temps.** Elle demande de structurer l'action des armées dans une organisation de commandement, des infrastructures, une RH formée et entraînée à ILI, et une doctrine.

Tout d'abord, les armées ont fait évoluer leur corpus doctrinal afin de construire une approche cohérente formalisée au sein de la Doctrine interarmées Influence et lutte informationnelle des armées (« DIA-10 ILI »).

Ensuite, l'intégration de la fonction influence passe également par un effort de formation aujourd'hui porté notamment par le CIAE de Lyon, afin de délivrer les compétences nécessaires au sein des états-majors. Il ressort des auditions menées que la priorité consiste à sensibiliser l'ensemble des personnels aux atouts et aux risques liés à l'influence. Ensuite, il s'agit de former des spécialistes capables de maîtriser la sphère informationnelle et de s'insérer utilement dans cet environnement de façon à le modeler en fonction des intérêts français. Ces spécialistes seront notamment en charge de la production de contenus, de narratifs ou de support. Au-delà de l'acquisition de compétences techniques, cela suppose également de comprendre l'audience ciblée et de maîtriser les codes culturels de la cible.

Par ailleurs, l'influence est progressivement intégrée aux scénarii des exercices dans une logique d'acculturation des personnels. À l'influence jouée dans le scenario, s'ajoute parfois une action d'influence réelle. En particulier, les grands exercices de type Orion ou Polaris, permettent à la fois de s'entraîner à la conception et à la mise en œuvre d'opérations d'influence, mais constituent également eux-mêmes des formes de « signalement stratégique » à destination des compétiteurs et des alliés. Les effets produits demeurent néanmoins difficiles à évaluer. Les exercices Pégase incarnent plus particulièrement cette fonction pour l'armée de l'air de l'espace. Ce sont des exercices de projection de puissance aérospatiale à très longue distance. Conceptualisés initialement dans le cadre de la contribution de l'AAE à la stratégie française dans l'Indopacifique, leurs résultats ont largement dépassé les attendus, selon les informations fournies à vos rapporteures. Par ailleurs, ces actions renforcent l'image de la France auprès des partenaires présents dans la zone. Ceci contribue fortement à développer des

partenariats stratégiques sur la route de l'Indopacifique vers les territoires d'outre-mer, grâce au concept « d'escales valorisées ». Selon les informations fournies par l'EMAAE, elles consistent en des escales dont le besoin technique n'est pas avéré, mais le passage prolongé sur place et une interaction dans le domaine aérien permet de cultiver la relation. La solidarité et la fiabilité de l'engagement français sont ainsi mieux incarnées et renforcés auprès de nos partenaires. En matière d'influence, faire dire à d'autres ce qu'on voudrait dire soi-même, mais avec les clés culturelles locales, constitue un objectif à rechercher. Le message n'en est que plus percutant. L'état-major opérations Air décline au niveau opératif et tactique cette directive et désigne l'équipe qui va piloter le volet influence dès la phase de planification de la mission. Une équipe prépare les narratifs, les contenus et les moyens de diffusion en bonne coordination avec les missions militaires de défense, qui constituent autant de relais potentiels. Enfin, l'influence générée par Pégase soutient les exports des matériels aériens de manière efficace.

ii. Les autres acteurs mobilisés au-delà du premier cercle

● Les actions menées dans le cadre de l'ILI sont distinctes des actions de communication ou de rayonnement menées par d'autres services du ministère des Armées. Ces dernières participent néanmoins au renforcement des actions d'influence.

S'agissant de la communication institutionnelle, vos rapporteures relèvent notamment un véritable effort de modernisation et de diversification des contenus de communication porté par la Délégation à l'information et à la communication de la Défense (DICoD). La portée stratégique de chaque message est mesurée, et de manière réciproque, chaque intervention dans les médias s'inscrit dans la déclinaison des objectifs de communication stratégique. Surtout, la DICoD veille à la cohérence d'ensemble de la communication du ministère des Armées, malgré un réel morcellement des capacités de communication (EMA COM, DGA COM, SGA COM, et les trois SIRPA d'armées), qui viennent dorénavant s'ajouter aux actions coordonnées par ASO dans le champ de l'influence. **Vos rapporteures, émettent donc un point de vigilance relatif à la préservation de la cohérence d'ensemble du dispositif, à mesure que la fonction influence et lutte informationnelle aura vocation à monter en puissance au niveau du ministère, mais également en interministériel.**

La DICoD joue également un rôle important en matière de veille et d'analyse comme de lutte contre les manipulations de l'information et de sensibilisation du grand public et des médias, à travers notamment la publication d'un guide de lutte contre la désinformation en juillet 2024, qui effectue une synthèse des bonnes pratiques à adopter pour lutter contre les ingérences numériques étrangères. Le guide aurait notamment été diffusé dans les classes de défense.

Enfin, la mission cinéma et industries créatives créée en 2016 participe également indirectement de la stratégie d'influence à travers l'accompagnement de près de 200 projets par an en moyenne, malgré des moyens limités en comparaison avec certains de nos alliés et compétiteurs. Ainsi, comme l'indiquaient déjà les rapporteurs de la mission d'information sur le rôle de l'éducation et de la culture dans la défense nationale, en mai 2024 « *Alors que son périmètre s'est élargi en 2019 à l'ensemble des industries culturelles et créatives, la MCIC ne compte actuellement que 7 effectifs. Son budget est inférieur à 100 000 euros, en dépit de sa nécessaire participation à de nombreux salons hexagonaux voire internationaux dans une perspective de rayonnement et d'influence*. » (1) En conséquence, les rapporteurs appelaient « *au renforcement significatif des moyens de la MCIC* » pour passer à l'échelle.

● Les missions de défense, qui dépendent de la DGRIS, constituent également un réseau de capteurs et de relais particulièrement important au service de la fonction influence.

iii. Les principaux défis rencontrés

Selon les informations fournies à vos rapporteures, les défis rencontrés dans l'opérationnalisation de la fonction influence sont principalement d'ordres culturel et capacitaire.

● D'une part, la prise en compte d'un nouveau champ de lutte ne va pas de soi. Les dimensions doctrinales et de formation sont prégnantes. Il faut continuer de faire évoluer la manière de réfléchir, l'analyse de la mission et la manœuvre qui en découle.

● D'autre part, il faut générer des viviers de spécialistes capables de conseiller le commandement, gérer un schéma capacitaire complexe au regard du nombre et de la nature très différente des équipements requis : du simple canon à son à l'application numérique la plus sophistiquée empruntant à l'IA générative.

C. UNE RÉPONSE NATIONALE QUI S'INSCRIT DANS UN ÉCOSYSTÈME EUROPÉEN ET INTERNATIONAL MARQUÉ PAR LA PROFUSION DES INITIATIVES AU RISQUE DE NUIRE À LA LISIBILITÉ DE LA RÉPONSE

1. Une mobilisation bienvenue face à une menace qui ne connaît pas de frontières

Bien que la lutte contre les manipulations de l'information et l'influence relèvent essentiellement d'une approche nationale, une réponse isolée ne peut permettre de lutter efficacement contre des menaces multiformes

---

(1) M. Christophe Blanchet et Mme Martine Etienne. Rapport d'information déposé en application de l'article 145 du règlement, par la commission de la défense nationale et des forces armées, en conclusion des travaux d'une mission d'information sur le rôle de l'éducation et de la culture dans la défense nationale, n° 2693, déposé le mercredi 29 mai 2024.

et mondialisées. La France peut néanmoins s'appuyer sur un réseau d'alliances et de partenariats dense, au premier plan duquel se trouvent l'UE et l'OTAN ; des organisations qui ont dorénavant pleinement saisi le défi que constituent les menaces hybrides. Les organisations internationales constituent en effet des enceintes particulièrement intéressantes pour partager l'état de la menace et créer des partenariats. Toutefois, vos rapporteures considèrent que si cette réponse peut être coordonnée, les États membres doivent rester souverains en la matière.

Si de nombreux progrès ont été réalisés, force est de constater que peu de partenaires sont en réalité dotés d'écosystèmes de lutte contre les manipulations de l'information aussi complets que celui dont dispose la France. Il ressort des auditions menées par vos rapporteures, notamment à Bruxelles et à Londres, que la France joue un rôle central et moteur en la matière. Un dialogue ambitieux existe notamment avec les Britanniques.

a. L'Union européenne : le rôle précurseur du SEAE en matière de lutte contre les manipulations de l'information

● **La prise en compte des menaces hybrides au niveau européen est relativement récente**. Les concepts de menaces et de stratégies hybrides sont devenus des sujets stratégiques majeurs à compter de 2014, après l'annexion de la Crimée par la Russie. Si l'OTAN a formellement reconnu les stratégies hybrides au sommet du Pays de Galles en 2014, l'UE, quant à elle, a officiellement adopté le terme de menace hybride dans ses documents en 2015, en réponse à l'utilisation par la Russie de stratégies hybrides en Ukraine. En avril 2016, l'UE a adopté un « Cadre commun sur la lutte contre les menaces hybrides », dans lequel elle décrit la combinaison de désinformation, de cyberattaques, de pressions économiques, et d'opérations militaires discrètes comme des menaces hybrides. Un code européen des bonnes pratiques contre la désinformation a également été établi en 2018, puis renforcé en 2022**,** afin d'inciter les plateformes en ligne à s'autoréguler et à coopérer avec la société civile pour valoriser les sources d'information considérées comme fiables. Il s'appuie sur une *task force* pluridisciplinaire composée à la fois d'acteurs institutionnels, de plateformes en ligne, de think tanks et de *fact-checkers* avec pour ambition de suivre les évolutions de la menace informationnelle.

● **L'UE et ses États membres se sont progressivement organisés pour faire face aux dangers représentés par les menaces hybrides, dont les manipulations de l'information d'origine étrangère, également appelées *foreign information manipulation and interference* (FIMI).** Le SEAE joue un rôle central dans les travaux actuels et a développé des outils pour soutenir l'action des États membres. En particulier, la division de la communication stratégique du SEAE, que vos rapporteures ont pu rencontrer, dirige les travaux sur la désinformation étrangère, les manipulations de l'information et les ingérences. Elle a pour mandat d'analyser l'environnement informationnel, afin de permettre la mise en œuvre de la politique étrangère de l'Union européenne et de protéger ses valeurs et ses intérêts. Les États membres de l'Union sont mobilisés pour renforcer le partage d'information sur les manipulations de l'information *via* des canaux dédiés

tels que le Système d'alerte rapide (*Rapid Alert System* - RAS), dont l'animation est assurée par le SEAE, destiné au partage entre les États-membres et les institutions européennes de données sur les campagnes informationnelles en cours et la coordination des réponses.

Chronologie des dispositifs de l'Union européenne en matière de lutte contre les manipulations de l'information

En 2015, une division StratCom (capacités de communication stratégique) a été créée au sein du SEAE, avec un mandat dédié à la veille des manœuvres informationnelles étrangères et au développement de la communication stratégique. Cela a conduit à la création d'un système d'alerte rapide (*Rapid Alert System*) qui permet aux États membres et aux institutions de l'UE de partager des cas de manœuvres informationnelles.

En 2018, la Commission et la Haute Représentante ont publié un plan d'action contre la désinformation, qui visait notamment à renforcer les moyens de la division StratCom du SEAE et à encourager les actions de sensibilisation des institutions européennes auprès du grand public.

En 2019, le groupe de travail horizontal du Conseil sur le « renforcement de la résilience et de la lutte contre les menaces hybrides » (ERCHT) a été mis en place afin de coordonner les travaux et la circulation de l'information entre le Conseil de l'UE et les États membres et mettre en œuvre des politiques et instruments cohérents de lutte contre les menaces hybrides.

En 2022, la Boussole stratégique de l'Union européenne a appelé à la création d'une boîte à outils de lutte contre les ingérences étrangères et manipulations de l'information comprenant des mécanismes de réaction, dont l'imposition de sanctions financières à l'encontre des acteurs se livrant à de telles activités.

En 2022, le Règlement sur les services numériques (« DSA ») a été adopté imposant aux très grandes plateformes et moteurs de recherche, l'évaluation des risques systémiques sur leurs services, ainsi que la mise en place de mesures d'atténuation pour y répondre. Ce règlement participe également à l'intégrité des processus électoraux et à la lutte contre les ingérences étrangères.

Dans le cadre de la Politique de sécurité et de défense commune (PSDC), l'Union européenne a mis en place des équipes de réaction rapide, regroupant des experts de différents pays pour répondre aux menaces hybrides (intégrant la lutte contre les manipulations de l'information) qui peuvent être déployées à la suite d'une requête d'un État membre pour répondre à une attaque menée sur son territoire.

Source : DGRIS en réponse au questionnaire de vos rapporteures.

Chaque année, le SEAE publie d'ailleurs un rapport sur les activités de manipulation de l'information et d'ingérence menées depuis l'étranger. L'édition 2025 introduit un nouvel outil pour l'analyse des manipulations de l'information et des ingérences provenant de l'étranger : la matrice d'exposition aux FIMI. Cette

matrice a été utilisée pour analyser un échantillon de 505 incidents FIMI impliquant environ 38 000 canaux actifs dans la manipulation de l'information. Comme les années précédentes, la Russie et la Chine restent des acteurs majeurs de la menace FIMI.

Toutefois, selon les représentants de la DGRIS auditionnés par vos rapporteures, la volonté de la Commission européenne de jouer un rôle plus important en ce qui concerne les menaces hybrides, et les manipulations de l'information en particulier, doit être accompagnée d'une coordination étroite, pour ne pas fragmenter l'action des institutions européennes en la matière. En effet, Ursula Von Der Leyen, a annoncé la création d'un « bouclier démocratique européen » pour lutter contre les campagnes d'ingérences numériques étrangères et renforcer la résilience et la préparation de la société.

Le Parlement européen prend également toute sa place dans le contrôle de cette nouvelle politique puisque, dans la lignée des travaux des deux commissions spéciales successives sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (INGE), a été créée en décembre 2024, une commission spéciale sur le « bouclier européen de la démocratie » (EUDS), présidée par Nathalie Loiseau.

Il ressort des auditions menées par vos rapporteures que les institutions européennes s'appuient également sur un écosystème de think tanks et d'ONG, comme le site au ton satirique EUvsDesinfo, qui réfute des contenus de propagande, pour renforcer la portée des actions de *debunking* et de communication stratégique menées.

● **L'UE apparaît également comme l'échelon adapté pour développer la réglementation d'un espace informationnel par nature non territorialisé**. Une lecture commune des enjeux liés à la régulation des plateformes a émergé grâce à l'élaboration du règlement pour les services numériques (*Digital Services Act*, DSA), aujourd'hui remis en question par certains acteurs de la *tech* américaine. Au-delà des mesures précédentes, le règlement européen sur l'Intelligence artificielle (IA Act) de 2024 vise à contraindre les « déployeurs » d'un système d'IA à informer les utilisateurs lorsqu'un contenu est généré ou manipulé par une IA, ce qui peut s'appliquer aux plateformes numériques (règlement UE 2024/1689 du Parlement et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle).

● **Enfin, une nouvelle étape a été franchie dans la réponse aux manipulations de l'information à travers l'adoption d'un nouveau régime de sanctions européen visant les attaques hybrides de la Russie.** Le 8 octobre 2024, l'Union européenne a adopté un nouveau régime de sanctions visant les acteurs de la déstabilisation russe - soit un spectre plus large que les seules manipulations de l'information, dont le premier paquet de sanctions a été entériné le 16 décembre 2024. Ce cadre permet à l'UE de cibler des personnes et des entités participant à des actions et des politiques menées par le gouvernement de la Fédération de Russie,

qui portent atteinte aux valeurs fondamentales de l'UE et de ses États membres, à leur sécurité, à leur indépendance et à leur intégrité, ainsi qu'à celles d'organisations internationales et de pays tiers. Les mesures restrictives liées aux attaques hybrides menées par la Russie consistent en des interdictions de pénétrer sur le territoire de l'UE visant des personnes physiques, en un gel des avoirs visant des personnes physiques et des entités, et en une interdiction de mettre des fonds ou des ressources économiques à la disposition des personnes inscrites sur la liste. Actuellement 16 personnes et trois entités sont concernées. Figurent notamment sur la liste l'unité 29155 de la GRU, une unité secrète au sein du service de renseignement de l'armée ou l'agence de presse *African Initiative*. Le 20 mai 2025, le Conseil a décidé d'imposer des mesures restrictives supplémentaires à l'encontre de 21 personnes et de 6 entités pour leur responsabilité dans des actions déstabilisatrices menées par la Russie à l'étranger. Des mesures visent spécifiquement les campagnes de désinformation et de manipulations de l'information**,** dont la suspension des activités de diffusion dans les États membres de l'Union européenne de *Sputnik*, *Russia Today*, *Rossiya 24*, *NTV*, *Rossiya 1*, *REN TV* et *Pervyi Kanal* jusqu'à ce que la guerre d'agression contre l'Ukraine prenne fin.

b. L'OTAN : une organisation efficace qui pourrait être remise en cause par la nouvelle administration américaine

● L'OTAN a su construire des capacités de communication stratégique, d'une part, et de lutte contre les manipulations de l'information, d'autre part. Néanmoins, les avancées réalisées semblent aujourd'hui remises en cause sous l'effet de la pression de la nouvelle administration américaine.

● L'efficacité de la défense collective assurée par l'OTAN repose sur la force et la détermination de ses pays membres. L'Organisation juge donc logique de se préoccuper des campagnes de manipulation et des ingérences dans la sphère de l'information, auxquelles se livrent les acteurs étrangers qui cherchent à affaiblir les pays de l'Alliance et donc à éroder sa capacité à protéger leurs populations. En outre, étant une alliance de pays démocratiques, l'OTAN tire sa légitimité de la confiance et du soutien que lui témoignent les citoyens de ses pays membres. Saper la confiance de la population contribue à affaiblir la solidarité de l'Alliance.

S'il convient de souligner que l'OTAN reconnaît pleinement la primauté de la compétence nationale pour répondre à toute activité hybride affectant une Nation, l'action de l'Alliance, en soutien à un Allié faisant face à une campagne hybride, se place dans le cadre de la défense collective.

● L'OTAN axe son approche sur les « menaces informationnelles », définies comme des activités de manipulation intentionnelles, préjudiciables et coordonnées qui sont menées par des acteurs étatiques et non étatiques dans le but d'affaiblir et de diviser l'OTAN, ses pays membres et ses partenaires. Les actes en question sont commis de manière délibérée et coordonnée par des acteurs étatiques ou non étatiques dans l'intention de manipuler le public ciblé, y compris par l'intermédiaire de tiers agissant depuis l'intérieur ou l'extérieur du territoire.

Pour les combattre, l'OTAN s'est dotée d'une boîte à outils qui comprend des mesures envisageables sur le court, le moyen et le long termes, y compris des mesures proactives. Ces mesures remplissent quatre fonctions clés : comprendre l'environnement informationnel (i) – les services de l'OTAN produisent notamment une « *situational awareness* » permettant d'identifier les pays de l'Alliance dans lesquels les actions doivent être menées prioritairement ; se prémunir contre les menaces informationnelles (ii) ; endiguer les incidents informationnels et en atténuer les effets (iii) ; et tirer les enseignements des menaces informationnelles pour être mieux armés (iv). La communication proactive est l'un des principaux outils de la lutte contre les menaces informationnelles. L'Alliance utilise divers canaux pour communiquer avec ses publics et leur fournir des informations exactes devant leur permettre de repérer les menaces informationnelles et de les déjouer.

Par ailleurs, l'OTAN dispose, comme le SEAE, d'un nouveau groupe de réaction rapide de l'OTAN (*NATO Rapid Response Group, NRRG*). Un centre d'excellence pour la communication stratégique se situe également à Riga en Lettonie, dont le rôle est de soutenir la communication stratégique de l'OTAN en fournissant notamment des analyses de manière à contribuer à l'amélioration des capacités de l'OTAN, de ses alliés et partenaires, en matière de communication stratégique.

● **Vos rapporteures seront particulièrement vigilantes à ce que ces avancées ne soient pas remises en cause.** En effet, il semblerait que le Secrétaire général de l'OTAN envisage de fusionner les fonctions de porte-parolat et de Secrétaire général chargé de la diplomatie publique, au risque de réduire les ambitions affichées et l'efficacité de l'action menée.

De fortes incertitudes quant au positionnement des États-Unis sur ces sujets se font jour, depuis la prise de fonction de la nouvelle administration. Une agence fédérale dédiée à la lutte contre les manipulations de l'information et les ingérences étrangères (*Global engagement center, GEC),* créée en 2016 au sein du département d'État va fermer définitivement sur demande de la nouvelle administration. Il semblerait que la nouvelle administration fasse de la défense de sa conception de la liberté d'expression un point cardinal de sa nouvelle approche diplomatique.

c. Des mécanismes internationaux nombreux

La coordination et le partage d'informations effectué dans les enceintes de l'UE et de l'OTAN s'accompagnent de l'existence de nombreux mécanismes internationaux de coordination en matière de lutte contre les manipulations de l'information.

Parmi les mécanismes principaux, peuvent notamment être cités le mécanisme de réaction rapide du G7 (*Rapid Response Mechanism*), au sein duquel l'OTAN est observatrice et le forum sur l'information et la démocratie, observatoire international prenant la forme d'un partenariat intergouvernemental réunissant 53 États démocratiques issus du pacte numérique mondial des Nations unies. Jouant le « rôle d'interface mondiale entre la recherche et la politique », le forum

ambitionne de devenir le pendant du GIEC. Cette dernière initiative est particulièrement intéressante en ce qu'elle souligne la nécessité d'inclure les pays du « Sud global » à la démarche de lutte contre les manipulations de l'information.

2. Une multiplication des concepts, des acteurs et des approches, qui nuit à la lisibilité d'ensemble de l'action menée

a. La nécessaire harmonisation des approches et des pratiques

Alors que les institutions européennes se montrent de plus en plus volontaristes en matière de lutte contre les manipulations de l'information, et tandis que les États-membres continuent de développer ou de renforcer leurs capacités nationales, **une accélération des efforts de rationalisation, de standardisation et d'homogénéisation au niveau de l'Union européenne s'avère nécessaire.**

● **En effet, il ressort des auditions menées par vos rapporteures que la multiplication des acteurs et des concepts nuirait à l'efficacité de l'action collective.**

Ainsi, certains observateurs mettent en avant un **manque d'harmonisation en matière de lutte contre les manipulations de l'information au niveau européen et une multiplication des acteurs** avec une « *diversité et superposition des périmètres qui pourraient à terme, nuire à la lisibilité de l'action collective et peut-être même finir par l'entraver* ». Les auteurs estiment ainsi qu'il « *semble nécessaire d'harmoniser les dispositifs, termes et pratiques » européens en matière de lutte contre les manipulations de l'information afin de faire émerger « une nouvelle approche communautaire* ». (1)

Le constat d'une approche européenne fragmentée est partagé par les auteurs du rapport intermédiaire de la commission spéciale du Parlement européen sur le bouclier européen pour la démocratie. Au-delà du renforcement des dispositifs existants comme le système d'alerte rapide du SEAE, les auteurs du rapport recommandent la création d'une agence dédiée à la lutte contre les manipulations de l'information sur la base du SEAE. Les auteurs suggèrent également de créer un cadre définissant des standards minimaux pour les États-membres et ainsi promouvoir des définitions communes, garantir l'interopérabilité et permettre l'identification de points de contact uniques dans chaque État-membre sur la question des FIMI.

---

(1) Blin, V., Naceur, Y. et Merer, J. (2025). Lutte contre les manipulations de l'information : la coopération européenne à l'épreuve de l'harmonisation des approches et pratiques. Revue Défense Nationale, 876(1), 27-34. (lien).

La proposition de création d'une agence unique fait écho à celle de la présidente de la Commission européenne, qui avait annoncé en juillet 2024 la création d'un « VIGINUM européen [(1)] » dans le cadre du nouveau bouclier démocratique. Néanmoins, selon les personnes auditionnées, il semble délicat qu'une entité européenne se substitue aux capacités nationales de détection et de réponse des États membres. La question de la protection des intérêts fondamentaux étant considérablement liée aux enjeux de souveraineté. Selon les informations fournies par VIGINUM, en lieu et place du projet d'agence européenne, la France serait davantage favorable à la création d'un **« centre d'excellence européen de lutte contre les manipulations de l'information »**, dont le cœur du mandat serait consacré à l'émergence d'une véritable communauté de la lutte contre les manipulations de l'information au sein de l'UE. Celui-ci pourrait notamment être chargé de partager des bonnes pratiques et méthodologies opérationnelles au sein de l'UE, notamment fondées sur l'analyse des comportements inauthentiques et la recherche en sources ouvertes et de renforcer l'interopérabilité entre les États-membres, afin d'améliorer la coopération et de permettre le partage de la connaissance sur la menace.

b. L'approfondissement de la coopération en matière de contre-hybridité

● Il ressort des auditions menées que le renforcement de la coopération en matière de contre-hybridité doit être poursuivi.

L'OTAN a réaffirmé le fait que les attaques hybrides pouvaient constituer un motif de déclenchement de l'article 5 du Traité de l'Atlantique Nord. Lors du Sommet de Varsovie en 2016, les Alliés ont publiquement déclaré qu'une attaque hybride contre un ou plusieurs Alliés pouvait être un motif d'invocation de l'article 5 du Traité de Washington. La position a été réaffirmée par le sommet de Vilnius en 2023 et de Washington en 2024. Néanmoins, l'on peut s'interroger sur la traduction concrète de cette ambition du fait de la difficulté à déterminer un seuil à partir duquel l'on pourrait considérer que des manœuvres informationnelles d'ampleur s'apparenteraient à de véritables actes de guerre, voire pourraient rentrer dans le champ de l'article 5 (défense collective) de l'OTAN ou l'article 42 § 7 du traité sur l'Union européenne (clause de défense mutuelle). **La stratégie sur le rôle de l'OTAN pour contrer les attaques hybrides adoptée en 2015 devrait d'ailleurs être mise à jour en 2025**. Celle-ci a pour but de « *faire en sorte que l'Alliance et les Alliés soient suffisamment préparés à contrer les attaques hybrides, quelles qu'elles soient* » et « *entend exercer une dissuasion propre à prévenir toute attaque de ce type contre l'Alliance et, si nécessaire, défendre les Alliés concernés* ».

● La coopération entre l'Union européenne et l'OTAN, en matière de lutte contre les menaces hybrides et en particulier contre les menaces informationnelles, pourrait être renforcée.

---

(1) Political guidelines for the Next European Commission 2024-2029, Strasbourg, 18 juillet 2024. (lien).

Selon les informations fournies par la DGRIS, la France a identifié la lutte contre les menaces hybrides comme un domaine prioritaire pour approfondir la coopération UE-OTAN et les deux organisations ont en effet comme priorité partagée de répondre à la campagne de déstabilisation menée par la Russie sur le continent européen et disposent d'outils et de compétences complémentaires pour atteindre cet objectif. L'OTAN, grâce à ses moyens militaires, est particulièrement bien placée pour améliorer l'appréciation de situation collective et contrer les manœuvres russes les plus hostiles. L'UE dispose d'outils indispensables en matière de sanctions, de protection des infrastructures critiques et de lutte contre la manipulation de l'information. La bonne coordination des réponses proposées par chaque organisation est nécessaire pour apporter une réponse efficace à ce défi de taille. Une récente note de l'IRIS recommande d'ailleurs de faire évoluer les accords de Berlin Plus du 14 mars 2003 en ce sens.

Le renforcement de cette coopération pourrait passer par le développement d'exercices communs, la création de canaux de communication pour mieux partager l'information, une meilleure utilisation du centre d'excellence UE-OTAN d'Helsinki, ainsi que le développement des synergies entre le Système d'Alerte Rapide (RAS) et le nouveau groupe de réaction rapide de l'OTAN (NRRG).

En 2017, a été créé le centre européen pour la lutte contre les menaces hybrides à Helsinki, au sein duquel l'UE et l'OTAN sont représentées. Ce centre permet de renforcer la résilience contre les menaces hybrides de ses membres par des formations et le partage d'analyses et de recommandations, ainsi que par des travaux conceptuels (à titre d'exemple, le concept sur les FIMI qui a été repris par l'UE et l'OTAN).

c. Des coopérations bilatérales à renforcer

● Si plusieurs coopérations ont été nouées, vos rapporteures estiment qu'il conviendrait de poursuivre le renforcement des coopérations à court et long termes avec les partenaires les plus vulnérables comme la Moldavie ou la Roumanie.

● La France, à travers son organisation construite autour de VIGINUM, fait figure de modèle pour nombre de partenaires européens.

En effet, en mars 2024, lors de son audition devant la commission d'enquête du Sénat sur les ingérences étrangères précitée, la directrice du centre d'excellence d'Helsinki sur les questions d'hybridité, indiquait, qu'à ses yeux, les deux États européens les mieux organisés pour faire face à ce type de menace sont la Suède et la France. Des liens ont notamment été établis avec l'Agence de défense psychologique de Stockholm à ce sujet. S'agissant des centres d'excellence de l'OTAN on peut également citer le centre d'excellence pour la lutte contre les menaces hybrides situé à Helsinki.

Compte tenu des importantes sollicitations et demandes d'assistance, VIGINUM a mis en place un programme de *capacity building* depuis 2024 et accompagne déjà plusieurs États européens cherchant à se doter de capacités similaires, à l'image notamment de la Moldavie.

● En complément, la France entretient des partenariats internationaux avec des pays affinitaires, dont notamment le Royaume-Uni, Singapour et l'Australie, afin de renforcer les réseaux existants ou d'en créer de nouveau pour lutter contre les stratégies hybrides. **Lors de leur déplacement au Royaume-Uni, vos rapporteures ont constaté que la partie britannique était favorable à approfondir la coopération avec la France en matière de lutte contre les menaces hybrides, y compris en l'incluant dans l'actualisation prochaine du traité de Lancaster House.**

Il convient également de noter que depuis février 2024 un format dédié dans le cadre du triangle de Weimar permet d'impulser des actions dans le cadre européen.

Vos rapporteures estiment que cette démarche de partenariat doit être poursuivie et intensifiée pour permettre à l'ensemble des partenaires qui le souhaitent de bénéficier de l'expérience de VIGINUM. Votre rapporteure Natalia Pouzyreff, qui s'est rendue en Moldavie, souhaite particulièrement insister sur la nécessité d'être en mesure de fournir des capacités techniques et des renforts d'experts détachés à court terme à nos partenaires les plus en difficultés. Compte tenu de la rapidité de la période électorale, la temporalité dans laquelle s'inscrit le *capacity building,* bien que bénéfique sur le long terme, peut s'avérer moins adaptée aux besoins.

Recommandation : Poursuivre et amplifier la construction de partenariats pour permettre à l'ensemble des partenaires qui le souhaitent de bénéficier de l'expérience de VIGINUM, en faisant un effort particulier sur les partenaires les plus fragiles.

II. EN COMPLÉMENT DES ACTIONS D'INFLUENCE MENÉES À DESTINATION DE L'INTERNATIONAL, LA NÉCESSITÉ DE RENFORCER LA RÉSISTANCE DE LA SOCIÉTÉ FRANÇAISE FACE AUX STRATÉGIES DE DESTABILISATION MENÉES PAR NOS COMPÉTITEURS

Au-delà des actions d'influence, il apparaît nécessaire à vos rapporteures d'être en mesure d'absorber les chocs et de résister à la désinformation. Donner moins de prise aux attaques et réduire nos vulnérabilités constitue une condition *sine qua non* pour élaborer une réponse efficace.

Tenant compte des limites de la stratégie française, vos rapporteures appellent à diffuser une véritable « culture de l'influence » au-delà des seuls ministères régaliens, mais, surtout, à agir en amont pour réduire les facteurs structurels de vulnérabilité face à la désinformation en veillant à associer davantage la société civile.

A. LES LIMITES DE LA STRATÉGIE D'INFLUENCE FRANÇAISE FACE AUX ATTAQUES DÉSINHIBÉES DE NOS COMPÉTITEURS CIBLANT LES INTÉRÊTS FRANÇAIS À L'ÉTRANGER MAIS ÉGALEMENT, DIRECTEMENT SUR LE TERRITOIRE NATIONAL

Les principales limites de la stratégie d'influence française résident d'abord dans l'asymétrie des moyens employés face à nos compétiteurs, dans son caractère essentiellement défensif, ensuite, et dans l'absence de vision commune et partagée, enfin.

1. Une asymétrie assumée face à nos compétiteurs : le respect de l'État de droit et des principes démocratiques

La première limite de la stratégie d'influence française est une limite assumée, qui tient au respect des principes et des valeurs démocratiques. Loin de constituer un obstacle, il convient d'en faire une force pour garantir un cadre équilibré entre régulation et préservation de la liberté d'expression.

En effet, si les compétiteurs de la France cherchent à déstabiliser les démocraties, la meilleure défense à leur opposer consiste à respecter les valeurs démocratiques, sans naïveté, mais sans les trahir. C'est d'ailleurs le principe qu'avait rappelé le Président de la République lors de la présentation de la RNS de 2022, lorsqu'il avait appelé à « *détecter et entraver* » la désinformation et les manipulations, « *mais à la manière d'une démocratie* ».

a. La fragilité, voire la relative impuissance, des États démocratiques face aux stratégies de nos compétiteurs et à l'instrumentalisation des réseaux sociaux

● Face aux actions désinhibées de nos compétiteurs, il convient de tenir compte des asymétries propres au champ informationnel et aux systèmes démocratiques, pour bâtir des réponses adaptées.

Dans un article paru dans la RDN, le Colonel Emmanuel Devigne revenait sur la double asymétrie caractéristique du champ informationnel (1) et les conséquences qu'elle emporte pour l'action publique.

D'une part, il existe une asymétrie propre à l'espace informationnel. Contrairement aux milieux traditionnels, la production d'effets peut difficilement être prédite ou anticipée. De plus, c'est un espace « privatisé » « *contrôlé par de grandes plateformes où le profit l'emporte sur l'éthique, très permissif où le coût d'entrée est très faible, où il n'existe pas réellement de droit à l'oubli*. » Par ailleurs, l'information n'est pas « une arme à effet dirigé » car elle évolue dans un espace dématérialisé et déterritorialisé, pouvant produire des effets collatéraux au-delà des

(1) Devigne, E. (2025). Les enjeux de la maîtrise de l'information dans les armées, une approche doctrinale. Revue Défense Nationale, 876(1), 66-74. (lien).

auditoires visés, ce qui constitue une difficulté importante pour l'action militaire. Cette asymétrie pose le défi de la cohérence dans les actions et les messages et celui de l'efficacité des actions dans un environnement où il n'existe pas de supériorité informationnelle : il s'agit au mieux de conquérir un « *avantage informationnel à un moment donné, sur des auditoires déterminés* ».

D'autre part, les démocraties ne jouent pas à armes égales avec les systèmes autoritaires, au sein desquels l'accès à l'information est verrouillé et caractérisées par le contrôle strict de l'opinion publique.

Les régimes démocratiques sont, par essence, plus vulnérables aux ingérences étrangères car ils doivent se conformer à des normes démocratiques et libérales qu'ignorent délibérément ceux qui cherchent à polluer leurs espaces informationnels. Parce qu'ils sont attachés à la liberté d'expression et au pluralisme des idées et des opinions, les espaces informationnels démocratiques sont par nature ouverts à la controverse, au débat contradictoire et même aux mensonges.

Ainsi, le recours à la désinformation demeure une « *véritable ligne rouge dans le concept militaire français* », tandis que « *la vérité demeure le fondement de notre crédibilité* ». Assumer cette asymétrie nécessite une grande cohérence d'ensemble et donc de penser la stratégie informationnelle à l'échelon interministériel. L'influence dépend de la cohérence entre une posture, une action physique et un message. En conséquence, déclarer des choses qui ne correspondent pas à sa culture ou à son action est souvent contreproductif. Lorsque ce qui est dit ne correspond pas à ce qui est fait, le risque de perte de crédibilité est majeur.

● L**'absence de souveraineté informationnelle accroît également la vulnérabilité du débat public dans les démocraties européennes, tandis que les grandes plateformes opèrent un revirement dans leur politique de modération des contenus.**

Ainsi, l'entreprise Meta a décidé le 7 janvier 2025, d'opérer un revirement complet de sa politique de modération des contenus sur les plateformes Facebook, Instagram et WhatsApp. Cette annonce implique notamment l'arrêt des partenariats avec les organisations de vérification des faits aux États-Unis. Selon les interlocuteurs rencontrés, cela pourrait ouvrir la voie à une décision similaire dans l'UE à plus ou moins long terme. Le cas échéant, cela constituerait une atteinte grave et immédiate à l'intégrité de l'espace informationnel européen et à la souveraineté démocratique de l'Union, sachant que ce programme finance des postes de « *fact-checkeurs* » pour certains médias, dont France Médias Monde.

Les médias traditionnels, notamment France Médias Monde, font également état d'une forme d'invisibilisation, de leurs contenus d'information par certaines plateformes de réseaux sociaux, au profit de contenus de divertissement ou de loisirs qui susciteraient davantage d'engagement de la part des utilisateurs ; ce serait notamment le cas sur les plateformes du groupe Meta. Ces phénomènes génèrent non seulement des pertes d'audience pour les médias

professionnels, mais ils favorisent aussi des « bulles de filtre » entre communautés affinitaires avec une polarisation et une radicalisation croissante des opinions, alimentées par la prolifération des fausses informations.

Les périodes électorales constituent en particulier des périodes de grande vulnérabilité pour les systèmes démocratiques, à l'image de l'instrumentalisation de Tik Tok dans le cadre des élections en Roumanie.

b. Le piège des procès en propagande et en censure – préserver l'équilibre entre régulation et liberté d'expression

● Dans cette guerre de l'information, il existe donc une iniquité des armes. Pour autant, la solution ne consiste pas à répliquer les mesures attentatoires à la liberté d'expression que prennent des régimes moins scrupuleux.

Deux écueils à éviter ont ainsi été résumés par Reporters sans frontières (RSF) dans une note adressée à vos rapporteures, d'une part, « *tomber dans le piège liberticide tendu par l'adversaire* » et, d'autre part, « *faire preuve de naïveté ou de mollesse dans la riposte* ».

C'est pourquoi, selon vos rapporteures, la France doit continuer de privilégier une approche de régulation par le mode de diffusion, tel que le fait aujourd'hui VIGINUM – c'est-à-dire par *les méthodes d'amplification ou d'altération* – et non par le contenu lui-même, car elle permet aux États démocratiques de préserver la liberté d'expression et d'éviter les accusations de censure. Censure qui provoque souvent des résultats inverses aux effets recherchés. Il convient avant tout d'éduquer, de sensibiliser et de dénoncer.

● La France peut aujourd'hui s'appuyer sur un cadre juridique équilibré pour lutter contre les manipulations de l'information.

Les réseaux sociaux sont extrêmement puissants et certains États prennent des mesures fortes, inédites. C'est le cas de la Roumanie, dont la Cour constitutionnelle a annulé le premier tour des élections présidentielles. L'exemple de l'Australie est aussi marquant, puisqu'une loi a été adoptée pour interdire aux jeunes de moins de 16 ans l'accès aux réseaux sociaux. Si la mise en œuvre de ce type de loi peut poser question, la symbolique est forte et souligne le choix politique fondamental qui se pose à nos démocraties.

La France dispose de plusieurs outils. La suspension de la diffusion de médias étrangers à l'instar des sanctions infligées par l'Union européenne à des médias russes constitue un des outils à disposition. Néanmoins, selon RSF, si elle peut se justifier sur le fond, l'interdiction de la diffusion de *Russia Today* et *Sputnik* en 2023 n'est pas une solution satisfaisante dans sa forme car elle sert le discours de légitimation de la censure dans les régimes autoritaires. Ces derniers peuvent, par exemple, alléguer qu'il y a équivalence entre *RT* et France 24 et, sur ce

fondement, adopter des mesures réciproques en fermant encore davantage leur espace informationnel aux médias indépendants.

Rappel du cadre juridique applicable à la lutte contre les manipulations de l'information

Les instruments de prévention

Tout d'abord, l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), est en mesure de rejeter une demande de convention de diffusion d'un service radio ou de télévision sur les réseaux de communications électroniques en cas de « *risque grave d'atteinte à la dignité de la personne humaine, à la liberté et à la propriété d'autrui, au caractère pluraliste de l'expression des courants de pensée et d'opinion, à la protection de l'enfance et de l'adolescence, à la sauvegarde de l'ordre public, aux besoins de la défense nationale ou aux intérêts fondamentaux de la Nation, dont le fonctionnement régulier de ses institutions* ». Elle dispose de ce pouvoir depuis la loi relative à la lutte contre la manipulation de l'information de 2018.

Les instruments de répression et d'entrave

L'article 27 de la loi du 29 juillet 1881 sanctionne pénalement la diffusion de fausses nouvelles de nature à troubler l'ordre public. Plus spécifiquement, l'article 411-10 du Code pénal sanctionne « *le fait de fournir, en vue de servir les intérêts d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger, aux autorités civiles ou militaires de la France des informations fausses de nature à les induire en erreur et à porter atteinte aux intérêts fondamentaux de la Nation* ».

Par ailleurs, le juge judiciaire peut être amené à ordonner la cessation d'« *allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité* » d'un scrutin électoral. Quant au juge administratif, il peut être saisi par l'Arcom afin de faire cesser la diffusion ou la distribution d'un service de communication audiovisuelle ne respectant pas les obligations françaises ou européennes d'interdiction de diffusion de contenus de services de communication audiovisuelle, notamment lorsqu'il s'agit d'une ingérence étrangère par la diffusion de fausses informations portant atteinte aux intérêts fondamentaux de la Nation.

Toujours en matière d'ingérences étrangères informationnelles, l'Arcom est également en mesure, depuis la loi relative à la lutte contre la manipulation de l'information de 2018, d'ordonner la suspension de la diffusion d'un service de communication audiovisuelle en période électorale, mais aussi de résilier unilatéralement une convention de service de communication audiovisuelle lorsqu'elle porte atteinte aux intérêts fondamentaux de la Nation. En outre, l'Arcom peut mettre en demeure les plateformes du numérique de retirer les contenus ou de faire cesser la diffusion des contenus interdits par une sanction de l'Union européenne. Pour ce qui concerne la propagande terroriste, l'Office anti-cybercriminalité (Ofac) peut enjoindre aux plateformes du numérique, sous le contrôle de l'Arcom, de retirer des contenus en ligne ou encore de bloquer des sites *Web*. Soulignons que le droit de l'Union européenne a renforcé ce dernier dispositif en établissant un délai d'une heure à compter de la réception de l'injonction de retrait pour les plateformes numériques.

Bien que le cadre juridique du champ informationnel se soit renforcé tant pour prévenir les manipulations de l'information affectant la sécurité et la défense nationale que pour les réprimer, il reste difficile pour les pouvoirs publics de faire face à la diffusion rapide de la désinformation et à la multiplicité des plateformes numériques. Les instruments juridiques de responsabilisation de ces dernières apparaissent alors déterminants pour agir au cœur de la désinformation dans une stratégie juridique de lutte informationnelle.

Les instruments de responsabilisation

En droit français, la loi relative à la lutte contre la manipulation de l'information de 2018 avait consacré une logique de responsabilisation des plateformes du numérique dans la gestion des contenus en ligne en obligeant ces dernières à mettre en œuvre, à leur niveau, des mécanismes de signalement et de modération de la désinformation sous la supervision de l'Arcom. Depuis l'adoption du règlement européen sur les services numériques de 2022 (DSA), cette responsabilisation a été harmonisée et renforcée à l'échelle de l'UE. Toutefois, ce règlement contraint les plateformes du numérique à mettre en œuvre des mécanismes similaires à la loi française de 2018 seulement contre la diffusion de contenus illicites, c'est-à-dire ceux qui ne sont pas conformes au droit de l'Union ou d'un État-membre. Autrement dit, la désinformation ne fait pas expressément l'objet d'une obligation de signalement et de modération, même si la notion européenne de « contenu illicite » peut, concerner les délits de diffusion de fausses nouvelles de nature à troubler l'ordre public ou à porter atteinte aux intérêts fondamentaux de la Nation. Le dispositif européen a donc allégé les contraintes des plateformes dans la lutte contre la désinformation au regard du droit français, d'autant plus que leur responsabilité juridique demeure limitée et qu'elles ne sont pas soumises à une obligation générale de surveillance des contenus en ligne ou de prendre des mesures à leur égard.

Enfin, la loi française du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique consacre une réserve citoyenne du numérique « *ayant pour objet de concourir à la transmission des valeurs de la République, au respect de l'ordre public, à la lutte contre la haine dans l'espace numérique et à des missions d'éducation, d'inclusion et d'amélioration de l'information en ligne* » et des dispositions visant à renforcer l'éducation au numérique et à la lutte contre la désinformation dans les établissements scolaires.

Source : mission d'information d'après Fadier, D. (2025). Les instruments juridiques de lutte informationnelle. Revue Défense Nationale, n° 876(1), 43-49. (lien).

● **Le recours à ces différents outils est néanmoins bien encadré pour préserver la liberté d'expression, garantissant la préservation d'un régime équilibré.** Par exemple, l'application TikTok a déjà été suspendue à titre conservatoire en Nouvelle-Calédonie, démontrant la possibilité de suspendre certains réseaux sociaux sous le contrôle du juge et à condition de respecter le principe de proportionnalité. Cette mesure avait été prise sur le fondement de la théorie des circonstances exceptionnelles, régime d'exception au droit commun, et a pris fin le 29 mai 2024. Néanmoins, en l'espèce, le Conseil d'État a jugé que la décision du Premier ministre de bloquer l'accès à TikTok ne respectait pas l'ensemble des conditions requises. Il relève notamment que l'interruption totale du service pour une durée indéterminée a constitué *« une atteinte disproportionnée à la liberté d'expression, à la liberté de communication des idées et opinions, et à la liberté d'accès à l'information ».*

2. Une stratégie qui demeure essentiellement défensive, en réaction aux attaques menées par nos compétiteurs

La deuxième limite réside dans le caractère essentiellement défensif des politiques mises en œuvre.

a. Le rôle de VIGINUM demeure limité à la détection et à la caractérisation des ingérences numériques étrangères

● Les missions de VIGINUM se limitent à la détection et à la caractérisation des ingérences numériques étrangères et n'incluent pas la production de contre-discours.

En effet, si le code de la défense confie au SGDSN, et à travers lui son agence VIGINUM, la mission de détecter les manipulations de l'information d'origine étrangère, en ce qu'elles menaceraient les intérêts fondamentaux de la nation, il n'est pas en charge de produire un contre-discours. Cette dimension relève avant tout de l'autorité politique.

Le service a été créé pour devenir le « *bouclier du débat public numérique français.* » S'appuyant sur un mandat clair issu du décret 2021-922 du 13 juillet 2021, la mission de VIGINUM est de caractériser les opérations d'ingérence numérique étrangère par des modes opératoires informationnels. Si le service dispose d'une capacité de réponse au travers des signalements de comptes ou l'exposition des campagnes étrangères, il ne lui appartient pas de riposter sur le plan informationnel. Selon les interlocuteurs rencontrés, le fait de ne pas faire de contre-discours protège VIGINUM d'accusations qui pourraient lui être faites d'incarner une forme de « Ministère de la Vérité » portant un jugement de valeur sur les opinions des citoyens. Le rôle de VIGINUM n'est pas d'attester ce qui est vrai ou ce qui est faux. Cette mission, essentielle pour une démocratie, doit avant tout reposer sur la société civile, les médias et le monde académique et scientifique. En revanche, le ministère de l'Europe et des affaires étrangères ainsi que le ministère des armées disposent du levier de la communication stratégique afin de rétablir les faits en cas d'accusation émanant de compétiteurs et des moyens de dénonciation publique.

En pratique, trois étapes peuvent être identifiées :

– La **caractérisation** d'une attaque ;

– **L'imputation technique** liée à l'emploi d'un mode opératoire (VIGINUM, COMCYBER, services de renseignement) ;

– **L'attribution :** si elle est rendue publique, il s'agit d'une décision politique.

Une fois la caractérisation opérée, VIGINUM adresse une note à l'interministériel à travers le COLMI, dont les membres décident ensuite de la réponse à adopter et de l'opportunité de dénoncer publiquement le mode opératoire

détecté. La dénonciation publique peut notamment se justifier lorsque le contenu manipulé a bénéficié d'une forte visibilité à l'image de la fausse vidéo d'un groupe terroriste menaçant d'incendier la cathédrale Notre-Dame de Paris. Lorsque la décision est prise, la réponse est souvent coordonnée et la parution d'un rapport public de VIGINUM est appuyée par une déclaration publique de niveau politique et d'un travail visant à médiatiser et organiser la diffusion au plus grand nombre des conclusions du rapport.

Les nombreux rapports d'information publiés par VIGINUM participent pleinement de la lutte contre la désinformation et de la sensibilisation du grand public à cette thématique. **Vos rapporteures tiennent à saluer la performance de VIGINUM. Le service a publié onze rapports en deux ans. Toutefois, encore faut-il que ces rapports soient lus et exploités au-delà des personnes déjà convaincues et acquises au sujet.**

b. Des efforts à poursuivre en matière de riposte et de réponse de court et de long termes

● Des efforts ont été réalisés afin de développer des actions de riposte et doivent être poursuivis.

Aujourd'hui, la réponse s'appuie sur un spectre d'actions allant du démenti, à la dénonciation publique, assorti éventuellement de sanctions et d'un signalement aux plateformes dans le but de suspendre les comptes concernés. Vos rapporteures se félicitent des avancées récentes en la matière depuis le discours du Président de la République du 5 mars à la télévision, dénonçant clairement la « menace russe » et son « agressivité ».

Par ailleurs, vos rapporteures notent avec satisfaction l'accélération des dénonciations publiques réalisées par le ministère de l'Europe et des affaires étrangères.

● Un des axes de progrès identifiés consiste en une plus grande opérationnalisation de la fonction riposte.

L'historien David Colon [(1)], auditionné par vos rapporteures, recommande de systématiser les ripostes, qui doivent être immédiates, simples et ludiques pour toucher une audience la plus large possible en donnant un caractère viral aux *debunkages* des campagnes de désinformation, en simplifiant les procédures de réponses et en recrutant des personnels plus familiers des réseaux sociaux et de leur fonctionnement pour assurer une communication plus efficace. Selon VIGINUM, tirant les enseignements de quatre ans de retour d'expérience opérationnelle, il convient également d'encourager une plus grande réactivité entre la détection d'une ingérence et la réponse apportée.

(1) La Guerre de l'information. Les États à la conquête de nos esprits, Paris, Tallandier, 2023.

● Si l'on constate une évolution de la posture de la France, qui hausse le ton face aux actions hostiles de la Russie et s'emploie à réagir plus rapidement, par des moyens y compris moins traditionnels, le recours à ce type de réponse doit être poursuivi et massifié.

Ainsi, la diplomatie française a attribué pour la première fois en avril 2025 au renseignement militaire russe (GRU) de nombreuses cyberattaques passées ; parmi lesquelles le piratage des *e-mails* de campagne d'Emmanuel Macron en 2017 ou encore l'attaque de plusieurs organismes dans le cadre des JOP de Paris 2024[(1)]. Le compte X de la présidence de la République a également pour la première fois démenti une fausse information relative à une vidéo du Président de la République sur les réseaux sociaux dans le train en direction de l'Ukraine, prenant dans sa main un mouchoir posé sur la table. En réponse à la rumeur d'un sachet de cocaïne qu'Emmanuel Macron n'aurait pas su cacher lors de son déplacement, l'Élysée a publié en guise de démenti un « mème », une image humoristique faite pour être partagée.

Vos rapporteures relèvent que le sarcasme constitue un registre rare pour la diplomatie française, qu'il s'agit d'une première pour le compte de l'Élysée et que le message, intervenu seulement quelques heures après que la rumeur ait commencé à être relayée, tranche également par sa réactivé [(2)]. L'on peut y voir une inspiration des méthodes ukrainiennes, qui dans le contexte de la guerre, ont été les premiers à répondre aux méthodes russes sur leur propre terrain.

● Ces pratiques ne sont pas entièrement nouvelles mais mériteraient d'être intégrées à une stratégie d'ensemble pour garantir la cohérence de la communication. Un article rapporte la manière dont le ministère de l'Europe et des affaires étrangères, à travers l'ambassade de France en Afrique du Sud avait réagi sur le réseau social X le 6 juin 2024 en réponse à une vidéo d'un pseudo-mercenaire français prétendument capturé en Ukraine, conseillant « *à vos comédiens de travailler leur accent avec quelques cours de français à l'Alliance française* [(3)]. » Toutefois, le recours à ce mode de réponse demeure soumis à la bonne volonté et à la personnalité de l'Ambassadeur sur place.

---

(1) Laureline Dupont et Eric Mandonnet, L'Express, « Comment Emmanuel Macron adapte sa stratégie face à la menace russe », 13 mai 2025. (lien).

(2) William Audureau, Le Monde, « Pour répondre à la rumeur du mouchoir, relayée par les sphères prorusses, l'Élysée a changé ses codes diplomatiques. », 15 mai 2025. (lien).

(3) « 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. » (lien).

Par ailleurs, il convient de s'assurer que le message soit également diffusé en anglais et par différents moyens de communication pour garantir que la riposte soit largement diffusée et, au besoin, partagée rapidement avec les partenaires pour amplifier sa portée.

Recommandation : S'assurer que les narratifs soient également diffusés en anglais et par différents moyens de communication pour garantir que la riposte soit largement diffusée et, au besoin, partagée rapidement avec les partenaires pour amplifier sa portée.

Selon les informations fournies à vos rapporteurs, le MEAE a lancé des chantiers structurants qui doivent être poursuivis :

– Une doctrine de riposte informationnelle à l'échelle du réseau a été définie sur la base de l'accompagnement d'une trentaine de postes et la constitution avec les directions géographiques et les postes de réseaux de rétablissement rapide des faits.

– La sous-direction veille et stratégie de la DCP a préparé avec VIGINUM les premières dénonciations publiques d'ingérences numériques étrangères contre la France.

La riposte est également portée avec l'état-major des armées. Ces actions de riposte sont conduites selon une gradation partagée avec la plupart des partenaires de la France et qui va du rétablissement des faits par un tiers, à la dénonciation publique assortie de sanctions en passant par le démenti officiel « *FAKE* ».

● Ces actions comportent néanmoins des limites importantes dans le cadre d'une stratégie se plaçant essentiellement en réaction à une attaque menée, au risque de générer des effets pervers lorsqu'une riposte à une tentative de manipulation de l'information rend en réalité la manœuvre informationnelle plus visible. Aussi, la lutte contre les manipulations de l'information et l'influence ne peuvent-elles exclusivement reposer sur une approche essentiellement réactive.

3. L'absence de vision commune et partagée affaiblit la stratégie française

La troisième limite de la stratégie d'influence française tient à l'absence de vision commune et partagée au niveau de l'État.

● Un des marqueurs les plus évidents réside dans l'absence de stratégie d'ensemble, capable de promouvoir une définition commune des concepts et des méthodes employées.

Alors que la RNS de 2022 prévoyait que la fonction stratégique influence s'incarnerait dans une « stratégie nationale d'influence » qui « *fixera le cadre général de l'action de l'ensemble des acteurs concernés, déterminera les intentions et permettra d'orienter les stratégies nationales sectorielles et/ou géographiques,* »

plus de deux ans après la publication de la RNS, force est de constater qu'aucune stratégie nationale d'influence n'a été publiée à ce jour, bien que la presse laisse entendre que le document serait déjà finalisé. (1)

Toujours selon la RNS, cette stratégie aurait pour objectifs de :

– défendre les intérêts de la France sur le temps long ainsi que les valeurs universelles, l'application du droit international, le multilatéralisme et la préservation des biens communs ;

– promouvoir et valoriser ses engagements dans tous les domaines ;

– répondre ou riposter à des manœuvres ou à des attaques, en particulier dans le champ informationnel, contre nos intérêts.

Interrogées sur l'absence de publication, les personnes auditionnées ont avancé que l'effort d'organisation et de structuration de l'écosystème l'avait certainement emporté sur l'élaboration d'une doctrine consolidée, résultant en une approche essentiellement empirique, pour parer aux attaques informationnelles subies par les armées, notamment en Afrique.

● Il ressort des auditions menées que l'approche empirique présente néanmoins de nombreuses limites et que l'absence de stratégie nationale d'influence complexifie l'action des ministères concourant à cette fonction stratégique, qui est perçue comme hautement sensible et politique.

Un des reproches régulièrement formulé consiste en l'absence d'effet final recherché (EFR) clairement défini, pour reprendre le vocable militaire. Une stratégie nationale établissant une définition commune, un périmètre défini, une répartition des responsabilités partagée entre tous, la création d'un mécanisme d'appréciation partagé de situation, de planification et de coordination interministérielle, permettrait d'apporter une cohérence haute à la fois dans l'approche narrative mais aussi dans les convergences des effets. Ainsi, dans la RDN précitée, le Colonel Devigne indiquait que malgré les progrès effectués la doctrine française demeurerait orpheline *« tant qu'une stratégie française d'influence n'est pas actée, avec des organes de commandement et de coordination interministériels adaptés. »*

● De la même manière, des disparités ont pu être constatées dans la mise en œuvre de la fonction, faute d'orientation claire.

Sur le territoire national, vos rapporteures ont notamment été alertées sur le fait qu'il n'existait pas encore d'harmonisation dans le rapport des services de presse des ministères aux *factcheckeurs*, chaque ministère adoptant une stratégie propre, résultant en des niveaux de réponse assez disparates.

---

(1) Elsa Trujillo, La Lettre, « La stratégie de lutte informationnelle suspendue au blocage politique », 4 septembre 2024. (lien).

À l'étranger, certaines ambassades apparaissent plus actives que d'autres. La politique menée semble restée très dépendante de la personnalité de l'ambassadeur.

Recommandation : Élaborer et publier une stratégie nationale d'influence clarifiant la définition des concepts et déterminant des priorités géographiques.

Vos rapporteures espèrent que l'actualisation de la RNS prévue en 2025 permettra de clarifier la fonction stratégique influence qu'elle avait instituée en 2022. La RNS pourrait ainsi servir de document cadre à d'autres stratégies plus sectorielles, définissant des objectifs plus précis comme la stratégie nationale d'influence ou de lutte contre les manipulations de l'information, à laquelle travaille aujourd'hui le SGDSN. Selon les informations recueillies par vos rapporteures pendant les auditions, la stratégie de lutte contre les manipulations de l'information vise à proposer une organisation rénovée et plus agile visant à mobiliser de manière plus efficace l'ensemble des instruments et incluant un volet résilience de la population.

En revanche, vos rapporteures mettent en garde contre le choix visant à évincer la fonction stratégique influence au profit de la seule stratégie de lutte contre les manipulations de l'information, car les deux politiques s'inscrivent dans un *continuum* d'actions, s'étendant du territoire national jusqu'à l'étranger et visant à garantir l'intégrité de l'espace informationnel, tout comme la défense des intérêts français.

Recommandation : Clarifier les contours et le portage de la fonction stratégique influence dans l'actualisation de la RNS de 2025.

Recommandation : Veiller à ne pas évincer la stratégie nationale d'influence au profit de la seule élaboration d'une stratégie de lutte contre les manipulations de l'information.

B. DIFFUSER UNE VÉRITABLE « CULTURE DE L'INFLUENCE » FRANÇAISE AU-DELÀ DES MINISTÈRES RÉGALIENS

À l'issue de leurs travaux, vos rapporteures ont acquis la conviction que l'influence, de la même manière que la lutte contre les manipulations de l'information, ne pouvait constituer qu'une politique transversale, devant infuser l'ensemble des politiques publiques, au-delà du seul champ régalien qui demeure néanmoins aujourd'hui le plus avancé dans l'opérationnalisation de la fonction. **À l'image du modèle britannique, il s'agit dorénavant de faire de l'influence « l'affaire de tous ».**

Vos rapporteures appellent donc de leurs vœux **l'élaboration d'une stratégie nationale d'influence visant à coordonner l'action des différentes administrations et partenaires au service de la politique d'influence.** En particulier, cette stratégie devra permettre d'envisager l'action de manière plus offensive et de prévoir des moyens à la hauteur des ambitions affichées.

1. Élaborer une stratégie nationale d'influence globale, assumée, excédant le seul champ des armées

a. Le besoin d'inscrire l'influence militaire dans un narratif national global et positif

● **Comme l'a rappelé le général de division Meunier, à la tête de la cellule anticipation stratégique et orientation (ASO) de l'EMA, l'influence est rarement strictement militaire.** La capacité à produire des effets dans le champ des perceptions dépend au contraire de l'intégration de l'action et de la posture des armées, dans une démarche cohérente avec l'action diplomatique et politique au sens large. Celle-ci relève notamment des champs culturels, économique, diplomatique, cyber et informationnel.

● **En outre, au-delà de l'action défensive ou réactive déjà mise en place, il convient de proposer un narratif au reste du monde**. Comme l'a résumé une personne auditionnée, « *si nous ne racontons pas notre histoire en tant que Français et européens, d'autres la raconteront pour nous*. »

À cet égard, le principal défi de la fonction influence réside dans la capacité pour les pouvoirs publics et, notamment le MEAE, en tant que chef de file de la fonction stratégique, à recréer un récit fédérateur qui puisse être exporté. Toutefois, seule une Nation sûre de son identité peut porter avec efficacité un message au monde. Le narratif doit ainsi se construire sur des valeurs positives et en temps de paix, autour de valeurs largement partagées. Auditionné par vos rapporteurs, le chercheur Laurent Cordonnier, directeur de la fondation Descartes, a insisté sur la nécessité de proposer un récit qui soit fidèle à la réalité, contrairement à celui de nos adversaires – *et en aucun cas de réécrire notre histoire ou de masquer son caractère pluriel*. Le récit pourrait ainsi insister sur des valeurs centrales de la République française comme l'universalisme, la laïcité ou encore le respect des libertés.

La tenue de grands évènements constitue à ce titre une opportunité importante pour consolider l'influence française à l'international. Il ressort des auditions menées que les Jeux olympiques et paralympiques de Paris 2024 sont apparus pour beaucoup comme un exemple réussi de cohésion nationale et de rayonnement. Comme le relève le CICDE, les stratégies informationnelles et d'ingérences numériques de nos adversaires n'ont, pendant cet événement et sur la période liée, que peu affecté la société française et n'ont pas imprégné l'espace numérique. Alors même que quelques semaines auparavant les manœuvres informationnelles et manipulations de l'information (punaises de lit, par exemple) trouvaient de l'écho et parvenaient à semer de la confusion, la réussite des JOP semble être venue effacer ces manipulations et empêcher que de nouvelles ne prennent de l'ampleur. Ainsi, selon le CICDE, lorsque les informations positives deviennent virales et occupent l'espace informationnel, que les citoyens se sentent partie d'un tout, unis derrière quelque chose de plus grand, alors les failles nécessaires au déploiement des stratégies de nos adversaires ne sont plus assez

importantes pour permettre l'efficacité et la réussite de ces dernières. La réponse vient donc aussi de la capacité à trouver un sens commun et des valeurs centrales autour desquelles peut s'inscrire et durer cette cohésion.

b. Un message unifié et mieux ciblé – le modèle britannique

● À titre de parangonnage, vos rapporteures se sont rendues au Royaume-Uni, souvent présenté comme un « modèle » en matière d'influence, à travers notamment l'importance donnée à la communication stratégique et le recours au secteur privé.

D'une part, les Britanniques ont pour réputation de posséder une « culture de l'influence » beaucoup plus intégrée, native, parfois qualifiée de « décomplexée ». Si toute comparaison avec un modèle étranger comporte nécessairement des limites, vos rapporteures retiennent notamment de leurs échanges le caractère parfaitement assumé des actions d'influence britanniques. Les campagnes de communication sont menées conformément aux grands principes du marketing : un message est spécialement conçu pour une cible donnée, un auditoire spécifique.

Les autorités n'hésitent pas à mobiliser l'ensemble des leviers et des relais à leur disposition, y compris privés, au service de la stratégie d'influence. La Grande-Bretagne dispose en effet, depuis longtemps, d'une culture profonde et assumée de l'influence. Aujourd'hui, celle-ci s'appuie sur un écosystème bien intégré entre les sphères publiques et privées, comme entre les sphères civile et militaire. En particulier, il semblerait que les Britanniques aient recours à certains acteurs privés pour mettre en œuvre leurs stratégies de communication sur le terrain (recherche, construction d'une stratégie, production de contenus, diffusion, etc.), ainsi qu'à des partenaires chargés de l'exécution (formation de journalistes, appui à la création de nouveaux médias ou création de contenu). L'on peut par exemple citer l'agence de communication *M&C Saatchi world services* ou l'ONG *Center for Information Resilience* s'agissant de la veille et de l'analyse. Les moyens humains et financiers consacrés à la Stratcom, selon le vocable britannique, sont très importants. L'on peut par exemple citer la campagne de soutien à l'Ukraine « *Ukraine : Frontline of freedom* » diffusée directement par le ministère de la défense britannique à destination de son opinion publique et, notamment du jeune public, pour renforcer le soutien à l'Ukraine.

D'autre part, leur capacité à diffuser un message unifié et cohérent, de manière coordonnée entre les différents services de l'État (élaboration d'un message unique, mise en marche de l'ensemble de l'appareil d'État au service de ce message) **a été mise en avant comme un atout de poids, tandis que la France semble souffrir en comparaison d'une trop grande dispersion des moyens,** voire est confrontée au défi du travail en silos, mais également à une moindre mobilisation des médias et des ONG, ce qui nuirait à l'efficacité de son message. Depuis 2018, les Britanniques ont théorisé cette organisation à travers le concept de « *Fusion*

doctrine (1) », qui prône une approche « *cross-government* » de la communication stratégique.

En matière militaire, les Britanniques peuvent s'appuyer sur une brigade dédiée à l'influence et aux actions psychologiques. Il s'agit de la 77e Brigade « *Information opérations* », recréée en 2015 sur le fondement d'une structure active lors de la Première guerre mondiale. Si peu d'informations précises sont disponibles sur ses actions, son rôle semble principalement de travailler en coordination avec les différents ministères et agences de l'État pour produire des effets à l'extérieur du territoire britannique mais également lutter contre la désinformation. La brigade serait composée en majorité de réservistes. Les autorités rencontrées ont insisté sur la nécessité de renforcer la mobilisation des réservistes en la matière mais également de faire tomber les barrières entre actions cinétiques et non-cinétiques.

● **Par ailleurs, le Royaume-Uni, confronté aux mêmes défis que la France, renforce la cohérence d'ensemble de son dispositif et s'emploie à mobiliser encore davantage son réseau diplomatique et militaire à l'étranger, face à l'accroissement de la menace informationnelle.**

En effet, la revue stratégique de défense britannique (SDR (2)) de mai 2025 met en avant la nécessité de développer une posture plus proactive et de désigner un point d'autorité unique pour coordonner l'action des unités spécialisées situées dans chaque armée, à travers notamment la création d'un commandement dédié (*CyberEM Command*), dans le but de réduire les doublons et d'accroître l'efficacité de l'action militaire. Ce commandement devrait agir à la manière d'un « *hub* » chargé de garantir la cohérence d'ensemble de l'action menée. La revue souligne également le rôle important que doit jouer la défense en soutien des campagnes de communication stratégique nationales.

Ce constat se traduit par la mise en place d'une politique visant à mieux structurer et à mobiliser le réseau de défense britannique à l'étranger. La SDR encourage le ministère des armées britannique à mobiliser tous les leviers à sa disposition pour développer des partenariats et protéger les intérêts britanniques. Comme en France, ces leviers devraient être matérialisés dans une nouvelle stratégie de diplomatie de défense (*Defence Diplomacy Strategy*) à paraître avant décembre 2025. La stratégie élaborée par le MOD, en lien avec les autres ministères et agences impliquées devra donner la priorité à l'utilisation de l'instrument de défense en appui de la politique étrangère au sens large. Surtout, des travaux en cours, présentés à vos rapporteurs lors de leur déplacement, visent à renforcer l'intégration du réseau militaire britannique à l'étranger (*Integrated Global Defence Network (IGDN*)) sous une même autorité pour une maximisation des effets et une plus grande agilité au service des intérêts britanniques. Le concept d'IGDN inclut notamment le réseau des attachés de défense, les bases à l'étranger, les centres d'entraînement, les personnels insérés, les officiers de liaison et conseillers insérés

(1) National Security Capability Review (2018).

(2) Revue stratégique de défense britannique p.123,(2025). (lien).

à l'étranger. Le Royaume-Uni peut en effet s'appuyer sur 8 500 personnels militaires et civils déployés à l'extérieur de ses frontières ainsi qu'un réseau d'attachés de défense permanents présents dans 91 pays.

Aussi, la SDR fixe-t-elle deux objectifs au ministère de la défense : la réalisation d'une revue de ses principales emprises à l'étranger afin d'en optimiser leur empreinte d'ici à avril 2026 et la création d'une filière professionnelle civile et militaire pour « l'engagement international de défense, » en encourageant une connaissance approfondie des régions présentant un intérêt pour le Royaume-Uni. **Le document recommande notamment que les voies d'accès aux postes de haut niveau soient conditionnées à l'exercice d'une mission à l'international, notamment à l'OTAN.**

Enfin, le Royaume-Uni semble favorable à une meilleure coopération avec ses alliés en la matière, au premier rang desquels la France, dans le cadre des accords de Lancaster House.

Recommandation : Accroître la coopération en matière hybride avec nos partenaires, en particulier approfondir notre partenariat avec les Britanniques.

● Tirant les leçons de l'exemple britannique, plusieurs axes d'effort peuvent être dégagés, afin de construire une véritable culture de l'influence française.

Au niveau militaire, il convient tout d'abord de poursuivre le renforcement de la mobilisation des attachés de défense. Selon les informations fournies à vos rapporteures, face à la multiplication des attaques informationnelles et des manipulations visant les forces françaises déployées à l'étranger, les armées ont renforcé les moyens de veille, d'alerte et de réponse.

Recommandation : Poursuivre la mobilisation des missions de défense à l'appui de la stratégie d'influence des armées, en s'inspirant du modèle britannique.

Par ailleurs, **vos rapporteures estiment qu'il conviendrait également de mobiliser davantage le réseau des officiers insérés,** de liaison, et des coopérants militaires, qui peuvent constituer autant de capteurs et de relais d'influence. Améliorer le suivi des *alumni* étrangers ayant bénéficié d'une formation militaire en France, pourrait également permettre de constituer un réseau particulièrement utile.

Recommandation : Renforcer la mobilisation du réseau des officiers insérés et de liaison ainsi que des élèves étrangers.

Un autre axe d'effort réside dans une plus forte mobilisation des relais d'influence et une meilleure valorisation des projets financés par la France dans le domaine culturel ou dans le cadre de l'aide au développement notamment. Alors qu'il s'agit d'une critique récurrente opposée notamment à la

politique d'aide au développement française, le ministère de l'Europe et des affaires étrangères s'emploie à y remédier. Selon les informations fournies à vos rapporteures, des instructions très claires ont été passées pour maximiser la visibilité des projets français. Néanmoins, l'enjeu est jugé plus profond : la communication institutionnelle traditionnelle visant à mettre en avant le financement de projets solidaires ne suffit plus. Les algorithmes des réseaux sociaux ne valorisent pas ce type de contenus institutionnels. Dans certaines zones, la défiance vis-à-vis de la parole publique est telle que la mise en avant des projets peut même se retourner contre le but poursuivi car cela expose nos partenaires qui sont ciblés par la désinformation et la diffamation. **Il s'agit de privilégier des campagnes de communication beaucoup plus fines, indirectes, pour créer de l'engagement et de l'impact sur les réseaux sociaux.**

Recommandation : En matière de communication à l'étranger, privilégier des campagnes de communication indirectes, pour créer de l'engagement et de l'impact sur les réseaux sociaux, en complément du recours aux relais institutionnels traditionnels.

Enfin, vos rapporteures considèrent également que les parlementaires pourraient davantage être associés à la déclinaison de la fonction influence. D'abord dans son contrôle bien sûr ; mais également en mobilisant davantage l'outil que constitue la diplomatie parlementaire.

c. Clarifier le pilotage et assumer les actions menées

La stratégie nationale d'influence doit ainsi permettre d'orienter et d'intégrer l'action des différentes administrations et d'articuler une approche globale dépassant le seul prisme militaire et intégrant tous les leviers de l'État, pour certains extérieurs à l'écosystème du COLMI (culture, justice, éducation).

i. Orienter et intégrer l'action des différents acteurs

● En matière de lutte contre les ingérences étrangères et de lutte contre les manipulations de l'information, **les auteurs du rapport sénatorial d'enquête sur la lutte contre les ingérences étrangères précité pointaient déjà un défaut de portage politique du Premier ministre,** s'agissant d'une stratégie pourtant fondamentalement 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.* » Or, l'existence d'une vision stratégique partagée au niveau de l'État semble nécessaire pour être en mesure de décliner cette vision et les messages associés dans chaque champ de l'action publique, en les faisant idéalement tous concourir à l'atteinte d'un même objectif et à la défense de narratifs communs.

Les auditions de vos rapporteures ont confirmé le constat d'une organisation qui fonctionne certes, mais qui demeure exposée au risque potentiel de morcellement ou de fonctionnement en silos. **Vos rapporteures estiment qu'il est néanmoins possible de se prémunir contre ces risques, du reste bien identifiés par les acteurs eux-mêmes, grâce à une comitologie efficace, placée sous la coordination du SGDSN.**

Ce constat est également partagé par David Colon qui propose une meilleure coopération et coordination à différentes échelles. À l'échelle nationale, la création d'une structure sous l'autorité directe du Président de la République est suggérée pour garantir la coordination de tous les acteurs concernés (COMCYBER, VIGINUM, CAPS, DGSE, DGSI, etc.), sous l'autorité d'une personnalité nommée par le Président de la République, pour décloisonner le système et permettre une meilleure efficacité de la réponse nationale.

● **Face au besoin de rationalisation de l'organisation déjà décrit *supra*, vos rapporteures considèrent néanmoins que le SGDSN gagnerait à voir son rôle de coordination conforté.** Le SGDSN, de par son positionnement auprès du Premier ministre, semble effectivement le plus à même de faire la jonction entre les deux stratégies, d'une part d'influence, et d'autre part, de lutte contre les manipulations de l'information.

En effet, le SGDSN assure d'ores et déjà le rôle de coordination face aux menaces hybrides. Il assure ainsi la présidence du comité opérationnel de lutte contre les manipulations de l'information (COLMI) mais également du comité opérationnel de liaison pour la sécurité économique (COLISÉ), du centre de coordination des crises cyber (C4), des groupes de travail sur les menaces hybrides (GT MH) et sur l'instrumentalisation du droit (*GT lawfare*), ainsi que de toute réunion interservices (RIS) *ad hoc* qui pourrait se tenir sur un sujet lié à l'hybridité. Son rôle de coordination est d'autant plus logique qu'il compte pour opérateur VIGINUM, chef de file en matière de lutte défensive contre la désinformation.

À ce titre, une récente étude de l'Institut Montaigne recommande de renouveler le pilotage stratégique en France en se dotant d'une structure comparable au *National Security Council* (NSC) ou du moins en renforçant le SGDSN, afin d'accroître la coordination de l'appareil d'État face aux crises [(1)]. L'institut Montaigne relève notamment que « *en France la distinction entre politique étrangère et politique de défense nationale génère des chaines fonctionnelles en silo et une difficulté à produire une réflexion transversale sur des sujets géographiques ou thématiques.* » À l'inverse, chez certains alliés, les NSC sont dirigés par un conseiller unique, proche du chef de l'exécutif et d'origine politique (et non administrative) comme en France.

(1) Jonathan Guiffard, Pour une administration stratégique de notre sécurité nationale. Institut Montaigne. 19 février 2025.

Recommandation : Conforter le rôle de coordination du SGDSN dans une logique de rationalisation de l'organisation interministérielle, afin d'assurer la jonction entre les deux stratégies, d'une part d'influence, et d'autre part, de lutte contre les manipulations de l'information.

ii. Le besoin d'une vision commune déclinable dans tous les champs de l'action publique

● **À terme, le risque informationnel, de même que les enjeux d'influence, doivent pouvoir être intégrés nativement à chaque politique publique, à la manière du risque cyber ou terroriste**. Toutefois, pour assurer la coordination d'ensemble de cette politique, une vision commune doit pouvoir être établie, puis partagée par l'ensemble des acteurs concourant à la stratégie d'influence.

Selon les personnes auditionnées, il est important d'impliquer l'ensemble des administrations mais également les collectivités territoriales, voire les entreprises. Chaque ministère est en réalité concerné : de l'Éducation nationale pour développer l'esprit critique, à la Justice pour développer des outils adaptés et efficaces de réponse judiciaire, au ministère de l'Intérieur pour préserver et renforcer la cohésion de la Nation en hexagone et outre-mer, au même titre que le ministère des affaires étrangères pour mobiliser les partenaires et les organisations internationales, voire que le ministère de la culture. S'agissant des entreprises, vos rapporteures sont convaincues qu'elles constituent des cibles privilégiées pour les stratégies de désinformation et que la politique du soutien export gagnerait à inclure un volet informationnel proactif. L'on peut, par exemple, citer la campagne de désinformation dont semble avoir été victime Dassault, relative à la perte alléguée d'un avion Rafale dans le cadre du conflit entre l'Inde et le Pakistan.

Aussi, **vos rapporteures sont-elles favorables à ce que puisse être menée une politique d'acculturation des agents publics dans les enceintes de formation de type INSP.** Afin de toucher un spectre plus large, l'IHEDN pourrait également être mobilisé, en incluant dans sa formation des modules dédiés.

Recommandation : Veiller à inclure la sensibilisation au risque informationnel et à l'influence au sein des formations des agents publics et à l'IHEDN.

● **Le développement d'une vision commune doit également permettre de rationaliser les initiatives existantes**. Vos rapporteures estiment ainsi que la refonte de la stratégie de communication de l'État, entreprise par le Service d'information du Gouvernement (SIG) afin de rendre la parole publique plus audible, mériterait d'être davantage coordonnée avec la montée en puissance de la fonction stratégique influence. De la même manière, la stratégie de lutte contre les manipulations de l'information doit permettre d'agréger les initiatives développées par chaque ministère, à l'image des annonces récentes du ministre de la Santé visant

à créer un observatoire dédié à la lutte contre la désinformation en santé [1]. Une plus grande cohérence d'ensemble doit ainsi être recherchée dans la communication de chaque ministère.

● Une meilleure intégration des ministères au-delà du champ régalien pourrait notamment se traduire par un élargissement du COLMI, qui demeure la principale instance de coordination interministérielle en matière de lutte contre les manipulations de l'information.

Il pourrait ainsi être envisagé d'inclure le ministère de la culture, de l'Éducation nationale (volet résilience de la Nation), voire de la justice – *qui bien qu'issu du champ régalien n'est pas aujourd'hui inclus systématiquemen*t- dans la comitologie issue du COLMI. Le lien avec le réseau des régulateurs, au premier rang desquels l'ARCOM, mériterait également d'être renforcé. Pour ne pas affaiblir la vocation opérationnelle du COLMI, l'association des autres ministères pourrait être ponctuelle ; la convocation d'un COLMI élargi, n'intervenant que lorsque la thématique traitée le justifierait. L'idée d'une gouvernance à géométrie variable avait d'ailleurs déjà fait l'objet d'une recommandation dans le rapport 2018 du CAPS et de l'IRSEM sur les manipulations de l'information [2]. Les auteurs constataient ainsi que les réseaux d'acteurs mis en place à l'étranger sont en général constitués d'un « noyau » à dominante sécuritaire (Affaires étrangères, Défense, Intérieur, renseignement) aux rencontres régulières et, en fonction de l'ordre du jour, d'un groupe élargi à d'autres ministères (Éducation, Culture, Justice), voire à des parlementaires et des acteurs de la société civile.

D'autres options pourraient également être envisagées pour mobiliser de manière permanente les différents ministères. La création de référents chargés de l'influence, différenciés ou non des fonctions de haut fonctionnaire de défense et de sécurité (HFDS), pourrait constituer une manière d'associer plus largement les ministères non régaliens, sur le modèle des travaux déjà menés par le SGDSN en matière de résilience nationale *via* l'intermédiaire de la commission interministérielle relative à la défense nationale (CIDN). Au-delà de sa participation à la comitologie interministérielle, le référent « influence » pourrait mener des actions de formation et de sensibilisation au risque informationnel en interne dans son ministère d'origine. Toutefois, il conviendrait de veiller à ce que ces personnalités disposent de profils adaptés avec un positionnement leur permettant d'essaimer dans leur organisation. À l'inverse, l'on pourrait également considérer que l'impulsion doit venir du niveau politique dans chaque ministère et ainsi décider de mener des actions de sensibilisation en priorité auprès des membres de cabinet, comme cela est déjà le cas au sujet des risques majeurs.

---

(1) Ministre de la Santé Yannick Neuder annonce la création d'"un observatoire pour lutter contre la désinformation en matière de santé". (lien).

(2) Rapport conjoint CAPS/IRSEM, « Les manipulations de l'information, un défi pour nos démocraties, septembre 2018. (lien).

Recommandation : Étudier l'opportunité d'élargir le COLMI à d'autres ministères y compris non régaliens (Culture, Éducation et Justice) et de créer un réseau de référents « influence » au sein des ministères pour s'assurer la bonne prise en compte de la fonction stratégique.

Les exercices interministériels de préparation aux crises gagneraient, en outre, à inclure systématiquement les enjeux de lutte contre la désinformation et de communication stratégique, afin de partager les bonnes pratiques.

2. Concevoir une doctrine de réponse claire

En cohérence avec la stratégie nationale d'influence à visée proactive, il convient de concevoir une doctrine de réponse claire en matière défensive.

a. Définir des seuils de réponse tout en veillant à ne pas rendre l'action prévisible

● **Alors que les actions de riposte demeurent largement empiriques, il ressort des auditions menées que la France gagnerait à davantage formaliser sa stratégie de réponse aux attaques informationnelles, au besoin en définissant des seuils qui permettront de guider la prise de décision en fonction du degré de dangerosité de la manœuvre informationnelle en cause.** Ces seuils auraient néanmoins vocation à évoluer et ne seraient pas rendus publics afin de ne pas prendre le risque de rendre la réponse prévisible pour nos compétiteurs.

Il s'agit effectivement d'un véritable enjeu de doctrine pour renforcer l'efficacité de la lutte contre les manipulations de l'information. La riposte doit s'inscrire dans une véritable stratégie d'ensemble au risque de tomber dans l'écueil du démenti permanent, qui peut s'avérer contre-productif et conduire à amplifier un contenu à l'origine peu visible. Ainsi, dans l'affaire précitée dite des étoiles de David, les comptes ayant publié les photos de la manœuvre ont eu en réalité peu d'impact à l'origine mais c'est leur reprise par les chaînes d'information en continu, puis par des membres du Gouvernement qui ont *in fine* contribué à donner de la visibilité à la manœuvre.

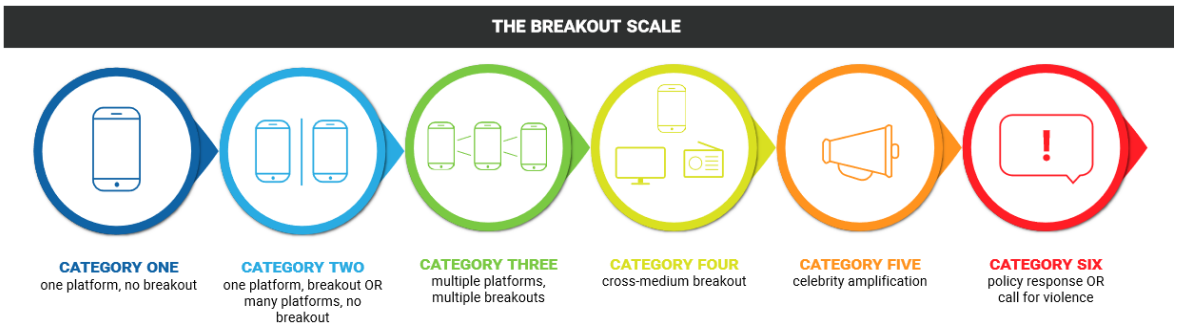
● **Pour définir des seuils de réponse, il convient néanmoins d'être en mesure d'évaluer l'impact potentiel d'une manœuvre informationnelle.** Si la mesure d'impact d'une attaque informationnelle demeure complexe, il semble nécessaire de concevoir des outils d'aide à la décision permettant de déterminer si la riposte est l'action la plus adaptée.

Comme l'indique VIGINUM en réponse à vos rapporteures, la mesure de l'impact d'une campagne numérique de manipulation de l'information ne fait actuellement pas l'objet d'un consensus au sein du monde académique. Principalement empirique, l'analyse de l'impact consiste souvent à relever des indicateurs quantitatifs de visibilité, fournis par les principales plateformes de réseaux sociaux (nombres de vues, de *likes*, de repartages ou de commentaires), mais ne fournissant qu'une vision parcellaire de l'exposition d'un lectorat ou d'un

auditorat à la campagne, sans permettre la mesure de ses effets sur le long terme. Ainsi, et en dépit de quelques rares outils disponibles, l'impact des manipulations de l'information en ligne sur les comportements des publics visés ou exposés demeure mal connu. Parmi ces outils, l'on peut notamment citer la *Breakout Scale* de Ben Nimmo (1), qui propose un cadre pour analyser la diffusion d'une fausse information en fonction du nombre de plateformes sur lesquelles elle est relayée et son degré de viralité. Il catégorise les opérations d'influence en six catégories, selon qu'elles parviennent ou non à dépasser la communauté (ou bulle) dans laquelle elles sont apparues, et suivant la nature des relais (médias grand public, personnalités reconnues) qui contribuent à la légitimer. À titre d'illustration, au niveau 1, l'information ne s'est propagée que dans sa communauté d'origine et sur une seule plateforme, alors qu'au niveau 6, elle a entraîné l'adoption d'une politique publique.

Néanmoins, elle ne préjuge pas de l'impact effectif de l'information sur un auditoire.

ÉCHELLE DE VIRALITÉ D'UNE FAUSSE INFORMATION



Source: Ben Nimmo, The breakout scale: Measuring the impact of influence operations, 2020.

Par ailleurs, VIGINUM développe un outil en propre appelé « VIGISCORE » qui doit permettre à terme de mieux mesurer le risque d'impact d'une campagne de désinformation avant d'agir. **Toutefois, face à l'absence de consensus sur un outil de mesure d'impact, il apparaît urgent d'accroître les travaux de recherche sur le sujet.**

● Enfin, **la doctrine de réponse doit ainsi être coordonnée au niveau de l'État et partagée au-delà du COLMI, même si elle demeure fortement dépendante aujourd'hui de l'autorité politique** ; seule décisionnaire *in fine* lorsqu'il s'agit de réagir publiquement ou d'attribuer une manœuvre.

Recommandation : Concevoir une doctrine de réponse claire en matière défensive et partagée au niveau de l'État, s'appuyant sur la définition de seuils de réponse, grâce à une meilleure connaissance de la mesure d'impact des stratégies de manipulations de l'information.

(1) Ben Nimmo, The breakout scale: Measuring the impact of influence operations, 2020. (lien).

b. Recourir à la déclassification de contenus de manière encadrée

● Dans le cadre de cette doctrine de réponse, la déclassification – ponctuelle et limitée – de contenus peut constituer un outil utile pour décrédibiliser l'action d'un compétiteur dans le cadre d'une manœuvre de riposte.

Déclassifier certains éléments pour ainsi permettre de pointer les contradictions et de mettre en évidence le caractère erroné d'un fait, à la manière des images de renseignement collectées par drone dans le cadre de l'affaire dite du charnier de Gossi, ou lorsque le ministre des Armées, Sébastien Lecornu a dénoncé vidéo à l'appui, les actions agressives d'un avion de chasse russe à l'égard d'un drone de surveillance français le 4 mars 2025 en Méditerranée orientale. Les autorités américaines ont d'ailleurs eu recours à la déclassification massive de contenus au début de la guerre en Ukraine – certes sans pour autant parvenir à éviter le conflit.

Recommandation : Recourir à la déclassification de contenus de manière encadrée à l'appui de la démonstration du caractère erroné d'une manipulation de l'information et dans l'objectif de décrédibiliser l'action d'un compétiteur dans le cadre d'une manœuvre de riposte.

● Plus largement, le recours à la déclassification de certains éléments constitue un outil à mobiliser pour renforcer la connaissance de la menace par le grand public.

Ainsi, aux États-Unis, l'agence du directeur du renseignement national (l'ODNI – *Office of the Director of national Intelligence*) publie un rapport annuel sur les menaces visant le pays, répertoriées par acteur ; que ces menaces soient ou non d'origine étatique (1).

Si un rapport bisannuel au Parlement sur l'état des menaces qui pèsent sur la sécurité nationale résultant des ingérences étrangères est déjà prévu par la loi du 25 juillet 2024 sur les ingérences étrangères, **vos rapporteures sont favorables à ce qu'il inclue également les ingérences numériques étrangères et dresse un état des lieux de la menace en matière informationnelle.**

Recommandation : Enrichir le rapport au Parlement prévu par la loi du 25 juillet 2024 sur les ingérences étrangères en y intégrant un état des lieux de la menace en matière informationnelle et en y incluant les ingérences numériques étrangères.

(1) Annual Threat Assessment Report of the U.S. Intelligence community. (lien).

c. Renforcer les sanctions : passer de la lutte contre les manipulations de l'information à la lutte contre les manipulateurs de l'information

● Au-delà des actions de riposte menées dans le seul champ informationnel, dont l'efficacité peut s'avérer limitée, il convient de mobiliser tous les leviers à disposition de l'État afin d'augmenter le coût des manœuvres informationnelles pour leurs auteurs. La perspective de sanctions renforcées ou d'entraves peut agir comme une forme de dissuasion à l'encontre des manipulateurs.

Il s'agit ainsi de passer de la lutte contre les manipulations de l'information, à la lutte contre les manipulateurs de l'information.

En effet, la réponse à une attaque hybride ne doit pas nécessairement être conduite dans le champ utilisé par l'attaquant. Mobiliser tous les leviers de l'État - *politique de visa, sanctions pénales et économiques, sanctions européennes, etc*. – doit permettre de dissuader et d'augmenter le coût de l'action pour nos compétiteurs.

Recommandation : Passer de la lutte contre les manipulations de l'information à la lutte contre les manipulateurs de l'information ; au-delà des actions de riposte menées dans le seul champ informationnel, renforcer les sanctions et mobiliser tous les leviers à disposition de l'État afin d'augmenter le coût des manœuvres informationnelles pour leurs auteurs dans une logique de dissuasion.

● Il ressort des auditions menées, que les outils juridiques semblent aujourd'hui suffisamment robustes, tant à l'échelon national qu'européen mais qu'ils pourraient être davantage utilisés.

Ainsi, la France met en place une réponse graduée allant jusqu'à l'entrave administrative et financière, récemment renforcée par les dispositions de la loi du 24 juillet 2024 visant à prévenir les ingérences étrangères [(1)]. L'État dispose d'une large gamme de mesures possibles en matière de contre-ingérence. Selon les informations fournies à vos rapporteures, outre les entraves administratives, ces dernières peuvent comprendre la mise en œuvre d'entraves diplomatiques qui relèvent d'une décision politique et qui sont mises en œuvre par le MEAE – *avec notamment des propositions de gels d'avoir et de sanctions au niveau de l'UE lorsque les individus ou personnes morales concernés entrent dans le champ de ces régimes*.

Des entraves judiciaires peuvent également être décidées lorsqu'une infraction est constituée, qu'elle relève des dispositions relatives aux atteintes aux intérêts fondamentaux de la Nation (intelligence avec une puissance étrangère, livraison d'informations à une puissance étrangère, sabotage), ou d'infractions de droit commun. Les infractions d'atteinte aux intérêts fondamentaux de la Nation permettent d'appréhender les actions dites de « haut du spectre », sans toujours permettre d'appréhender les formes modernes d'ingérence, qui visent à tisser des

(1) LOI n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France.

relations personnelles avec des agents publics ou des acteurs politiques, ou à mobiliser plusieurs intermédiaires comme les *proxies*.

La loi du 24 juillet 2024 visant à lutter contre les ingérences étrangères en France a cependant donné à l'État de nouveaux outils pour répondre à cette menace :

– en instaurant une nouvelle obligation déclarative à l'égard des acteurs d'influence agissant pour le compte de mandants étrangers ;

– en étendant le dispositif de gel des avoirs aux personnes morales et physiques se livrant à des actions d'ingérence sur le territoire national(1);

– en introduisant une nouvelle disposition dans le code pénal (article 411-12) qui érige en circonstance aggravante le fait de commettre certains crimes et délits de droit commun dans le but de servir les intérêts d'une puissance étrangère.

Selon les informations fournies par la direction des affaires criminelles et des grâces (DACG), ce dernier dispositif devrait permettre d'apporter une réponse pénale plus adaptée aux infractions dites du « bas du spectre » et pourra être utilisé contre les actions de basse intensité (par exemple dans le cas du tag type étoiles de David ou des mains rouges) commises notamment par des *proxies* des services de renseignement. Toutefois, la nouvelle qualification ne semble pas avoir été mise en œuvre pour l'instant. Il convient de poursuivre le travail important de **sensibilisation et d'acculturation** des magistrats aux qualifications spécialisées permettant d'appréhender pleinement ces menaces hybrides. Selon les informations fournies à vos rapporteures, les services ont également sensibilisé très largement les services de police et de gendarmerie à la nécessité de signaler en temps réel des cas considérés comme suspects au regard d'une grille de plusieurs critères. **Pour autant, si ces actions se multipliaient, le risque est celui d'une saturation, qui est sans doute aussi l'effet recherché par la Russie.**

Par ailleurs, il peut être relevé que **l'article L. 562-1 du code monétaire et financier** définit désormais l'acte d'ingérence comme « *un agissement commis directement ou indirectement à la demande ou pour le compte d'une puissance étrangère et ayant pour objet ou pour effet, par tout moyen, y compris par la communication d'informations fausses ou inexactes, de porter atteinte aux intérêts fondamentaux de la Nation, au fonctionnement ou l'intégrité de ses infrastructures essentielles ou au fonctionnement de ses institutions démocratiques*. »

---

(1) Cette mesure était jusqu'alors exclusivement applicable en matière de terrorisme. L'article L.562-1 1°bis du code monétaire et financier vise également, désormais, les « actes d'ingérences », définis comme les « agissements commis directement ou indirectement à la demande ou pour le compte d'une puissance étrangère et ayant pour objet ou pour effet, par tout moyen, y compris par la communication d'informations fausses ou inexactes, de porter atteintes aux intérêts fondamentaux de la Nation, au fonctionnement ou à l'intégrité de ses infrastructures essentielles ou au fonctionnement régulier de ses institutions démocratiques ». Ce dispositif national, plus large que le dispositif européen qui ne vise que la Russie, existe de façon autonome par rapport à ce dernier.

Cependant, il convient de souligner que cette définition **n'est pas donnée par le code pénal**, mais par le code monétaire et financier, dans le cadre du nouveau dispositif administratif de gel des avoirs étendu aux ingérences étrangères. Cette définition n'apparaît pas à l'article 411-12 du code pénal qui encadre la nouvelle circonstance aggravante en lien avec les ingérences étrangères.

En effet, selon les informations fournies par la DACG, la frontière ténue entre influence et ingérence (la première pouvant mener à la seconde, voire s'y superposer) aurait pu constituer une difficulté en matière pénale si le législateur avait fait le choix de créer une infraction *sui generis* d'ingérences étrangères qui aurait supposé de définir très précisément un phénomène qui, cela a été rappelé, peut s'avérer particulièrement nébuleux et protéiforme.

Le choix d'opter plutôt pour la création d'une circonstance aggravante permet de contourner cette difficulté : en effet, par principe, cette circonstance vient aggraver des faits constituant une infraction principale. La nature répréhensible du comportement est donc établie. La circonstance aggravante requiert simplement un élément intentionnel supplémentaire, à savoir que le crime ou le délit a été commis « *dans le but de servir les intérêts d'une puissance étrangère, ou d'une entreprise, ou d'une organisation étrangère ou sous contrôle étrangère* ».

Selon la DACG, le choix de la circonstance aggravante plutôt que de l'infraction autonome permet ainsi d'éviter toute ambiguïté quant à une éventuelle pénalisation excessive d'un comportement qui pourrait être autrement qualifié d'influence ; de surcroît, c'est un outil juridiquement plus facile à manier pour les magistrats, qui n'ont pas à démontrer un ensemble d'éléments constitutifs d'une infraction autonome. Enfin, son champ d'application large permet d'appréhender la quasi-totalité des atteintes aux personnes et des atteintes aux biens.

Ainsi, si la définition des ingérences étrangères prévue par le code monétaire et financier peut éventuellement éclairer l'application de la circonstance aggravante en matière pénale, elle en reste distincte et a essentiellement vocation à permettre la mise en œuvre du dispositif administratif de gel des avoirs.

S'il existe un débat autour de la création d'une infraction spécifique d'ingérence informationnelle, vos rapporteures estiment qu'il est prématuré au regard des risques qu'il pourrait entraîner.

S'agissant plus précisément de la création d'une **infraction spécifique aux ingérences en matière informationnelle,** il s'agissait d'une proposition émise dans le cadre du projet de loi « renseignement » pour laquelle la direction des affaires criminelles et des grâces avait émis un avis réservé. Cette proposition était motivée par l'idée que le dispositif pénal actuel ne permettrait pas d'appréhender de façon satisfaisante certaines situations dans lesquelles de fausses informations sont diffusées sur le territoire français pour le compte d'une puissance étrangère.

La DACG a émis un avis réservé sur une telle proposition, pour trois séries de raisons :

– cette infraction semble en tout ou en partie redondante avec des dispositifs déjà existants, et notamment certaines infractions pénales (délits de presse ou infractions du livre IV du code pénal en matière d'intelligence avec une puissance étrangère) ;

– les exigences constitutionnelles en matière d'atteinte à la liberté d'expression sont très élevées, si bien que la création d'un délit de diffusion de fausses informations apparaît délicate et doit être entourée de garanties telles que cela prive la répression de tout intérêt en pratique ;

– sur le plan opérationnel, la création d'une telle infraction semble préjudiciable à la cohérence des entraves.

Au demeurant, **le recours à la circonstance aggravante, plutôt qu'à l'infraction dédiée, autorise une grande facilité d'utilisation dans le traitement judiciaire**, puisqu'elle est susceptible d'assortir la quasi-totalité des infractions d'atteintes aux personnes et d'atteintes aux biens, là où une infraction spécifique d'ingérence étrangère en tant que telle nécessiterait la démonstration d'éléments constitutifs particuliers. En outre, une telle infraction dédiée risquerait d'entrer en concours avec des infractions existantes, notamment les atteintes aux intérêts fondamentaux de la nation, venant ainsi brouiller la lisibilité du dispositif répressif en la matière.

Cadre juridique applicable en matière d'ingérence numérique étrangère

En matière d'ingérences étrangères numériques, VIGINUM favorise la fluidification de l'échange d'informations entre les services de renseignement et l'autorité judiciaire et la bonne articulation des leviers d'entrave, qu'ils soient administratifs ou judiciaires. Les mesures mises en place en matière administrative permettent de lutter en amont contre ce phénomène et visent autant les organisations étatiques à la manœuvre en détectant et limitant leurs mouvements, que leurs moyens d'action, en les neutralisant.

Le procédé de judiciarisation piloté par VIGINUM suit ensuite les étapes suivantes :

Identification et caractérisation de l'ingérence étrangère numérique : une fois que VIGINUM a identifié et caractérisé les auteurs de manipulations de l'information ou d'ingérences numériques, les informations sont transmises aux autorités compétentes, notamment les services de renseignement qui qualifient les évènements, les imputent à des organisations étatiques puis évoquent les situations avec l'autorité judiciaire en application de l'article 40 du code de procédure pénale (CPP). Il est difficile de produire des données chiffrées sur la judiciarisation de ce type d'ingérences car tous les *« incidents »* détectés ne sont pas judiciarisés et il existe une grande perméabilité entre les groupes d'attaquants dans le cyberespace.

Enquête judiciaire : le parquet, une fois informé, peut décider d'ouvrir une enquête de flagrance, préliminaire ou bien une information judiciaire auprès d'un magistrat instructeur. VIGINUM peut également répondre à des réquisitions judiciaires dans le cadre d'enquêtes pénales : cela a notamment été le cas dans le cadre de l'enquête sur les étoiles de David. Sur réquisitions, VIGINUM a pu produire des notes détaillées qui passent par le comité éthique et scientifique, comportant en annexes, les données concernées.

Poursuites pénales : si les éléments de procédure le permettent, les poursuites pénales peuvent être engagées contre les auteurs identifiés. La section cyber du parquet de Paris est un interlocuteur privilégié de VIGINUM en matière d'ingérence étrangère numérique. La combinaison du nouvel article 411-12 du CP et de l'article 706-72 du CPP, issus de la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France, confie à la section cyber du parquet de PARIS, J3, au travers de sa compétence nationale concurrente en matière de cybercriminalité, une compétence en matière d'atteintes aux intérêts fondamentaux de la nation.

Coopération Internationale : dans le cas d'investigations portant sur les ingérences étrangères numériques, des demandes d'entraide judiciaire active (à d'autres pays) peuvent être délivrées et des actions communes d'interpellations peuvent être coordonnées avec des partenaires internationaux.

Sanctions encourues : les auteurs peuvent faire face à diverses sanctions, allant des amendes à des peines de prison, en fonction de la gravité des infractions commises.

Source : DACG, Ministère de la Justice

● Outre les poursuites judiciaires, pour certains dossiers, le nouveau régime de sanction européen qui vise « les acteurs de déstabilisation russe » a été décrit comme un outil pertinent par les personnes auditionnées.

La France apporte également une réponse diplomatique et politique à la menace portée par certains services de renseignement adverses particulièrement offensifs, au travers de mesures de rétorsion diplomatique (déclaration *persona non grata*, par exemple*)* à l'encontre de leurs représentants non déclarés sous couverture diplomatique. La France pourrait également soutenir la restriction des visas des diplomates russes afin de marquer sa ferme condamnation des stratégies hybrides russes.

● S'agissant de l'application des outils existants, il semble encore trop tôt pour établir un bilan des dispositions prévues par la loi du 25 juillet 2024 visant à prévenir les ingérences étrangères en France. À ce stade, compte tenu du caractère extrêmement récent de l'entrée en vigueur de ce texte, la direction des affaires criminelles et des grâces ne dispose pas de suffisamment de recul pour évaluer la mise en œuvre de ce texte. Cependant, il semble clair que ce texte est venu combler un véritable besoin sur le plan des qualifications juridiques, afin que les magistrats puissent prendre en compte de façon satisfaisante les menaces hybrides, à la hauteur du danger qu'elles représentent, et en allant au-delà des seules qualifications relatives aux atteintes aux intérêts fondamentaux de la Nation.

Vos rapporteures ont interrogé les services du ministère de la justice sur les enquêtes en cours.

Selon les informations fournies :

– S'agissant des tags d'étoiles de David découverts à Paris : le 27 octobre 2023, un couple, de nationalité moldave, est interpellé, après la découverte de tags d'étoiles bleues, sur des façades d'immeubles dans le X^{e} arrondissement de Paris. Quelques jours plus tard, dans la nuit du 30 au 31 octobre 2023, d'autres étoiles taguées ont été découvertes dans le sud de Paris, en Hauts-de-Seine et Seine-Saint-Denis. Un autre couple, également de nationalité moldave, est repéré grâce aux caméras de surveillance.

Les trois enquêtes, ouvertes à Bobigny, Nanterre et Paris, pour « dégradation du bien d'autrui aggravée par la circonstance qu'elle a été commise en raison de l'origine, la race, l'ethnie ou la religion » ont été regroupées et le parquet de Paris a ouvert une information judiciaire. 7 ans d'emprisonnement sont encourus pour ce type de faits. S'agissant du couple interpellé sur les premiers faits, en situation irrégulière l'un et l'autre, ils ont été conduits au centre de rétention administrative. La procédure judiciaire a donc été classée en raison d'une « sanction d'une autre nature », c'est-à-dire « leur expulsion du territoire » d'après le parquet de Paris.

Le 9 novembre 2023, le Ministère de l'Europe et des Affaires étrangères produisait un communiqué indiquant que la France condamnait avec fermeté l'implication du réseau russe *Recent Reliable News* (*RRN/Doppelgänger*) dans l'amplification artificielle et la primo-diffusion sur les réseaux sociaux des photos des tags représentant des étoiles de David dans le 10^{e} arrondissement de Paris. En ce qui concerne leur amplification, VIGINUM a détecté le 6 novembre 2023 l'implication d'un r**éseau de 1095 bots** sur la plateforme X (anciennement Twitter), ayant publié 2589 posts contribuant à la polémique liée aux étoiles de David taguées au pochoir dans le 10e arrondissement de Paris. VIGINUM a considéré « avec un haut degré de confiance » que ces bots sont affiliés au dispositif RRN dans la mesure où une de leurs activités principales consiste à réorienter vers des sites internet du dispositif RRN.

– S'agissant de l'affaire des « mains rouges » taguées : dans la nuit du 13 au 14 mai 2024, 35 tags représentant des mains rouges avaient été peints sur le Mur des Justes au Mémorial de la Shoah à Paris. Le parquet de Paris a ouvert une information judiciaire et émit un mandat d'arrêt européen à l'encontre de trois suspects. À l'été 2024, ceux-ci ont été appréhendés en Croatie et en Bulgarie. L'un d'entre eux a accepté son transfert en France en août 2024 et a été placé en détention provisoire. Les suspects sont visés par une enquête pour « dégradation du bien d'autrui commise en réunion » avec circonstance aggravante, du fait qu'ils « ont été commis en raison de l'appartenance vraie ou supposée à une ethnie, race ou religion ». Sont encourus sept ans d'emprisonnement.

Source : DACG, Ministère de la Justice

● Afin de renforcer la lutte contre les auteurs des manipulations de l'information, des actions pourraient également être renforcées concernant le financement des manœuvres de déstabilisation.

Ainsi, le rapport NewsGuard/Cosmore (1) estime que 2,6 milliards de dollars annuels sont générés chaque année par les sites de désinformation grâce aux recettes publicitaires qu'ils perçoivent d'annonceurs. En ce sens, un encadrement et une régulation plus stricte de la publicité en ligne pourraient contribuer à restreindre le financement des campagnes d'influence et des opérations de désinformation.

3. Envisager l'action de manière plus offensive sans renier les valeurs démocratiques

● **Au-delà des actions de riposte déjà détaillées *supra*, il ressort des auditions menées par vos rapporteures, qu'il est nécessaire d'envisager l'action de manière plus proactive, voire offensive.**

Le chef d'état-major des armées, lui-même, incite à adopter une posture plus offensive : « *Il faut s'opposer à l'adversaire dans l'ensemble des champs où il nous attaque, en particulier dans le champ informationnel. On ne peut pas se contenter de démentir des manipulations par un communiqué officiel. Il faut aussi répondre là où la menace s'est révélée et là où elle a eu un impact. On peut faire un communiqué sur les punaises de lit… Mais si le message s'est propagé sur les réseaux sociaux, c'est aussi sur les réseaux sociaux qu'il faut intervenir pour informer et rétablir la vérité. Nous devons contrer l'ennemi là où il opère.* ***Nous devons être capables de nous défendre et éventuellement de conduire des actions dans l'espace informationnel adverse****. Ces actions doivent permettre de diffuser de l'information et toucher l'opinion publique de nos adversaires*. » (2)

● Ce constat est issu des différents retours d'expérience des conflits en cours. L'expérience des armées en Afrique et sur le flanc est de l'Europe montre qu'une posture défensive strictement limitée à une posture réactive ne peut constituer une stratégie efficace. Par nature, un terrain informationnel déserté profite aux narratifs de l'adversaire. **Les stratégies gagneraient donc à articuler à la fois des volets offensifs et défensifs, notamment pour éviter à nos compétiteurs de prendre l'avantage informationnel.**

La guerre en Ukraine démontre ainsi la manière dont les militaires ukrainiens ont perfectionné l'emploi de leurres ou le recours à des manœuvres d'intoxication et à la ruse (3). En effet, si les caractéristiques de la guerre évoluent, marquée notamment par une transparence accrue du champ de bataille, ruses et opérations de déception demeurent des outils indispensables. À titre d'exemple, la multiplication des leurres permet d'augmenter la survivabilité des unités tout en forçant l'adversaire à gaspiller des munitions coûteuses.

---

(1) Matt Skibinski, Newsguard, "Rapport : La publicité sur les sites de mésinformation ». (lien).

(2) Général Thierry Burkhard au Figaro: « En cas de désengagement américain, la défense européenne s'adaptera », Le Figaro, 10 novembre 2024.

(3) Ruses et opérations de déception dans la guerre d'Ukraine (2022-2024), Remy Hemez. Article paru dans la revue DSI n° 176, mars-avril 2025.

● Certains observateurs appellent ainsi à la réhabilitation des concepts de ruse et de déception. Par exemple, le Colonel Devigne [(1)] appelle de ses vœux un « *retour à la culture de la ruse* » afin de conserver la liberté d'action de la force militaire dans un contexte de transparence accrue du champ de bataille, qui passerait par le renforcement des capacités à « *savoir tromper la chaîne de commandement ennemie* ».

Selon les informations fournies, le développement des capteurs sur le champ de bataille génère une forme de transparence qui réduit la liberté des actions des forces sur le terrain. Retrouver la culture de la ruse doit permettre de dégrader la compréhension de l'ennemi pour l'inciter à réagir d'une manière préjudiciable à ses propres intérêts et réduire ses capacités de riposte. L'influence est au cœur de cette logique d'aveuglement de l'ennemi pour créer l'incertitude et gagner l'initiative. L'esprit de ruse doit permettre d'appuyer la manœuvre militaire et de sortir de la simple idée de manœuvre de diversion pour rentrer dans une logique de déception, au travers d'un panel beaucoup plus large de modes d'actions allant de la dissimulation (camouflage, contre-renseignement, sécurité cyber), à l'intoxication (orientation, amplification, manipulation) en passant par la simulation (diversion, leurrage, démonstration).

En effet, dans un environnement où la supériorité informationnelle semble hors d'atteinte, l'efficacité des actions réside davantage dans le fait d'obtenir un avantage informationnel à un moment donné, sur des auditoires déterminés. Pour les armées, y parvenir est un défi qui s'inscrit à la fois dans le temps long et qui s'adresse directement aux imaginaires de l'auditoire. Dès lors, « dire » ne suffit plus dans un monde dominé par les émotions, il faut « faire dire », avec la volonté d'agir plus efficacement sur le plan cognitif. L'ascendant informationnel passe à la fois par l'approfondissement de l'approche psychologique des auditoires, et par la capacité à manœuvrer dans l'espace informationnel au travers d'unités dédiées et dotées de moyens technologiques de dernière génération.

Selon les informations fournies à vos rapporteures, l'avantage informationnel se manifeste selon deux dimensions distinctes, chacune répondant à des objectifs spécifiques et complémentaires.

D'une part, la dimension stratégique, qui repose sur la domination des narratifs, a pour objectif d'imposer un cadre de perception favorable. Cette approche repose sur des actions cohérentes et coordonnées. Elle se matérialise notamment par la diffusion de messages structurés, le recours à des relais d'influence et la mise en place de campagnes informationnelles marquées ; l'ensemble contribuant à asseoir une position dominante dans le champ cognitif.

D'autre part, la dimension tactique se traduit par la domination de l'appréciation situationnelle sur le champ de bataille. Elle vise à dégrader la compréhension adverse tout en optimisant la prise de décision propre. Elle repose

---

(1) Devigne, E. (2025) . Les enjeux de la maîtrise de l'information dans les armées, une approche doctrinale. Revue Défense Nationale, n° 876(1), 66-74. (lien).

sur une manœuvre intégrée exploitant l'ensemble des compartiments de l'espace informationnel, combinée à une utilisation systématique de la ruse sous diverses formes. On retrouve ici les grands modes d'action de la déception : simulation, dissimulation, intoxication. L'accélération de la boucle renseignement-feux et une forte mobilité tactique permettent ainsi de maximiser l'efficacité opérationnelle, en privant l'adversaire de sa capacité d'anticipation et d'adaptation.

● Toutefois, le recours à de telles manœuvres ne peut s'envisager que dans un cadre légal bien délimité.

Les deux conditions d'efficacité doivent demeurer la véracité – la France ne fait pas d'inauthentique – et la cohérence de l'action à tous les niveaux – des actions inscrites dans le cadre d'une stratégie nationale, avec un narratif clair, dans une logique d'intégration interministérielle pilotée. Il en va de la crédibilité de l'action sur le temps long. Si certaines actions du fait de leur nature, sont secrètes, elles demeurent assumables.

En application du droit des conflits armés, la ruse est autorisée, pour tromper l'adversaire, mais la perfidie est proscrite. Ainsi, la France assume déjà le recours à des actions proactives dans le cyberespace selon un cadre d'engagement opérationnel clair. Selon les informations fournies à vos rapporteures, cela peut aller de la dénonciation des incohérences ou mensonges de l'adversaire à la conduite d'opérations dites de déception, c'est-à-dire de ruse, en induisant un adversaire en erreur, ou à la conduite d'actions de contre-influence. En revanche, la perfidie consisterait par exemple à usurper l'identité d'une entité protégée comme une ONG telle que la Croix-Rouge, alors qu'un exemple de ruse serait de laisser se diffuser le mauvais horaire de départ d'un convoi militaire. Les narratifs développés par la France sont authentiques et loyaux, sans chercher à nuire aux États, à désinformer leurs citoyens ou encore à déstabiliser leur société. Ce sont des narratifs efficaces adaptés aux auditoires ciblés.

● Il ressort des auditions menées qu'il existe un véritable besoin d'une vision politique claire et définie pour guider les actions des administrations concernées. Au regard de la grande sensibilité du sujet, vos rapporteures appellent de leurs vœux un débat associant les parlementaires, visant à déterminer les contours de l'aspect offensif de la stratégie d'influence. La conduite d'action d'influence offensive ne pourra s'affranchir d'une réflexion sur l'encadrement éthique nécessaire.

Aussi, l'association des parlementaires, pourrait-elle être actée dans l'élaboration de la stratégie nationale d'influence. Il s'agirait de définir notamment des limites dans le caractère offensif des actions menées et de déterminer les modalités de contrôle de l'action du Gouvernement dans une matière par nature secrète pour être efficace.

La production de contenu et leur diffusion pose notamment question. **Un des points qu'il semble notamment prioritaire de trancher réside dans l'éventualité du recours aux entreprises privées au service de la stratégie d'influence,** notamment s'agissant du recours aux outils publicitaires et marketing qui permettraient de rendre plus visible et de diffuser plus efficacement les contenus produits sur les réseaux sociaux, à la manière de la stratégie marketing d'une entreprise privée. **Si le recours à des prestataires permettrait d'amplifier les actions menées, il conviendrait néanmoins de veiller à ce que les entreprises concernées bénéficient d'un très haut niveau de confiance et ne travaillent pas pour d'autres gouvernements.**

Recommandation : Organiser un débat associant les parlementaires, visant à déterminer les contours de l'aspect offensif de la stratégie d'influence et notamment le possible recours à des prestataires privés.

4. Poser la question de l'adéquation entre les moyens et les ambitions

La stratégie nationale d'influence doit enfin et surtout clarifier la question de l'adéquation entre les moyens et les ambitions affichées.

Alors qu'un des enjeux principaux réside dans le passage à l'échelle des actions qui demeurent aujourd'hui encore trop échantillonnaires, la question des moyens est dimensionnante. **Cela demande des arbitrages clairs qui doivent reposer sur la détermination de priorités géographiques et thématiques.**

a. Des besoins humains et capacitaires

S'il est difficile d'identifier avec précision les moyens actuellement dédiés à la fonction influence du fait de leur dispersion, il ressort des auditions menées que les défis principaux dans le cadre de l'opérationnalisation sont d'ordres humains et capacitaires.

● **S'agissant du ministère des Armées, si les armées poursuivent leurs efforts pour augmenter les ressources humaines formées, les ressources dédiées à l'animation de cette fonction restent, elles, en revanche, comptées.** Ainsi, auditionnée par vos rapporteures, la cellule ASO dispose d'une équipe de 11 collaborateurs, dont 5 stagiaires civils. Par ailleurs, les spécialistes doivent être en mesure de traiter les auditoires cibles sur différents continents en fonction des opérations et des missions. Selon les informations fournies à vos rapporteures, l'opérationnalisation de la fonction l'influence va se poursuivre en faisant un effort sur la professionnalisation de certaines filières spécifiques et sur le recrutement et la formation des militaires qui opéreront dans le domaine de l'influence lors des opérations. Ces spécialistes sont en charge de la production de contenu, de narratifs ou de support, ou de leur supervision.

Vos rapporteures appellent par ailleurs de leurs vœux l'identification d'une filière « influence et lutte informationnelle » et sa valorisation dans les parcours de carrière militaires.

Recommandation : Identifier plus clairement une filière « influence et lutte informationnelle » et la valoriser dans les parcours de carrière militaires et rendre obligatoire un passage dans les organisations internationales pour accéder aux plus hautes fonctions.

● Par ailleurs, les spécificités de l'espace informationnel mettent en lumière l'enjeu du suivi du rythme des évolutions technologiques et un besoin de matériels à conception duale.

Parmi les besoins identifiés au niveau du ministère des Armées, figurent notamment des capacités de veille, de diffusion massive de messages sur des supports très variés, des ondes aux supports papier et numériques, afin de favoriser l'usage de relais de messages au sein des auditoires visés. Sur le champ tactique, les besoins portent sur des moyens de leurrage physique et thermique mais également sur des moyens drones ou laser par exemple, pour renforcer la capacité à porter des messages de l'autre côté d'une ligne de front.

L'un des enjeux centraux est celui de la démultiplication des effets à tous les niveaux (stratégique, opératif et tactique). Il ressort des auditions de vos rapporteures que l'épaisseur de chaque levier de l'influence reste à consolider au regard de la menace. **Le principal enjeu réside ainsi dans le passage à l'échelle.**

● De la même manière, il apparaît absolument nécessaire de poursuivre le « réarmement » du réseau diplomatique.

La réforme en cours de la direction de la communication et de la presse du ministère de l'Europe et des affaires étrangères y contribue directement et doit être menée à son terme. Une première étape devrait consister en la consolidation rapide des missions de planification et de conduite d'une communication d'influence de la sous-direction veille et stratégie. La communication élaborée doit s'avérer beaucoup plus ciblée pour toucher les publics visés de manière efficace, y compris au sein du réseau diplomatique.

Aujourd'hui, selon les informations fournies à vos rapporteures, les Ambassadeurs ont l'instruction de coordonner la stratégie de communication au niveau local, en s'appuyant sur « *tous les moyens de l'équipe France, y compris ceux des missions de défense* ». **Toutefois l'enjeu réside dans l'impact et les moyens à disposition, notamment de production vidéo, qui font aujourd'hui défaut.** Un appel à projet annuel aurait été ainsi en place par le ministère de l'Europe et des affaires étrangères pour financer les projets innovants des ambassades, dotés d'un budget de 500 000 € par an. L'enjeu reste néanmoins pour les ambassades de recruter des profils rompus à l'influence et à la communication au sein des services presse, tandis que ces missions sont bien souvent assurées par des profils *juniors* ou des VIA. À terme, ces personnes doivent pouvoir constituer les correspondants naturels des équipes de la direction veille et stratégie à Paris, disposant d'outils de

veille et en mesure faire remonter rapidement des informations et de participer à la diffusion efficace des narratifs en activant et en animant des réseaux et en identifiant des relais d'influence. Selon les informations fournies à vos rapporteures, seule une vingtaine de postes auraient été obtenus pour l'ensemble du réseau à date pour remplir les missions de communications et d'influence.

Vos rapporteures seront vigilantes à ce que les postes des services presse soient confortés, ce qui suppose de recruter et de former des personnels aptes à maîtriser les nouveaux canaux de communication, mais également de renforcer les moyens de communication stratégique à leur disposition notamment en matière de production de contenu et de diffusion.

Recommandation : Renforcer les moyens relatifs à la communication stratégique des services presse des ambassades et de la DCP, en faisait porter les efforts sur le recrutement de profils spécialisés dans les stratégies d'influence, afin de passer d'une communication institutionnelle à une véritable communication d'influence.

Afin d'augmenter les capacités, la RNS 2025 envisagerait, par ailleurs, la création d'une « réserve diplomatique citoyenne » pilotée par l'académie diplomatique et consulaire (1 000 personnes d'ici fin 2025). **Vos rapporteures considèrent que cette initiative est bienvenue car de nature à démultiplier les effets des actions menées à l'étranger mais ne doit pas se substituer aux efforts de réarmement du réseau diplomatique.**

● La France doit également pouvoir s'appuyer sur un audiovisuel public fort, à la hauteur des ambitions de la stratégie nationale d'influence.

Les médias français qui réalisent des audiences à l'étranger n'ont pas vocation à soutenir l'action française à l'international mais à en rendre compte avec impartialité, indépendance et honnêteté. Ils contribuent à leur manière, par leur éthique, leur professionnalisme, à faire exister un modèle d'information fiable et indépendante et de promouvoir ce modèle partout dans le monde. Les soutenir, c'est soutenir ce modèle. Ils participent d'une logique indirecte de rayonnement.

Selon la directrice générale de France Médias Monde, Marie-Christine Saragosse, auditionnée par vos rapporteures, il existe « *un besoin vital de moyens pour éviter le désarmement informationnel de la France.* » France Médias Monde porte une information libre, indépendante, équilibrée et qui lutte contre les manipulations de l'information et les fausses informations - en particulier celles ciblant la France – en français et dans vingt autres langues.

Le projet de contrat d'objectifs et de moyens 2024-2028 de France Médias Monde (FMM) avait vocation à préserver, sur la période, le périmètre de ses missions tout en développant ses nouveaux projets à l'international, de manière à faire face aux urgences qui se jouent à l'échelle mondiale. Toutefois, la trajectoire qui lui était associée a été remise en cause dès 2025 dans le projet de loi de finances - *avec un écart de 9,9 millions d'euros, ramené ensuite à 7,9 millions d'euros, lors du débat parlementaire*. Selon les informations fournies à vos rapporteures, FMM

dispose en 2025 d'une dotation publique de 273,1 millions d'euros, bien inférieure à celle de ses homologues internationaux (485 M€ pour *BBC World Service*, 450 M€ pour *Deutsche Welle*, sans compter les médias internationaux russes, chinois ou encore panarabes qui investissent 6 à 8 milliards d'euros dans leurs audiovisuels extérieurs, selon les informations transmises par FMM).

Aussi, **vos rapporteures estiment-elles qu'il est indispensable de conforter les moyens financiers alloués à l'audiovisuel extérieur de la France et que ces réflexions mériteraient d'être portées dans l'élaboration de la stratégie nationale d'influence.**

Recommandation : Consolider les moyens de l'audiovisuel public à la hauteur des moyens consacrés par nos alliés et en tenant compte du désengagement américain.

● Plus largement, il ressort des auditions menées par vos rapporteures qu'il convient de poursuivre le renforcement et l'optimisation des capacités de veille, de détection, et de caractérisation pour identifier plus rapidement les menaces et être en mesure de réduire le temps de réaction.

Cela passe en particulier par le renforcement des moyens à disposition de VIGINUM dont les actions sont actuellement limitées par des moyens comptés.

Le service dispose aujourd'hui un budget de 3,02 millions d'euros [(1)] en autorisations d'engagement et d'un effectif de 59 ETP, alliant des compétences diverses : ingénierie informatique, science de la donnée, analyse géopolitique, marketing digital, investigation numérique, etc. Si le budget semble relativement satisfaisant pour répondre aux missions actuelles du service, les besoins se font essentiellement sentir en matière RH. Une seule personne est actuellement chargée des partenariats avec la société civile, deux de ceux avec l'étranger. La formation de la société civile (notamment des médias), l'information du grand public et des entreprises, l'assistance à fournir aux partenaires étrangers du service ainsi que l'innovation continue sur l'IA nécessiteront des moyens supplémentaires. Si lors de leur visite de VIGINUM, vos rapporteures ont été sensibilisées au fait qu'il convenait de ne pas rigidifier la structure afin de conserver une forme d'agilité, à l'horizon 2027, le besoin exprimé par le service est de 80 agents, soit environ vingt agents de plus dédiés pour les deux tiers aux partenariats et pour un tiers aux activités de *data science*.

Recommandation : Renforcer les moyens humains à disposition de VIGINUM à hauteur de 20 ETP supplémentaires, en particulier s'agissant des fonctions de partenariats et d'ouverture sur la société civile.

(1) Hors dépenses de Titre 2.

b. La nécessaire clarification des objectifs et la définition de priorités géographiques et thématiques

● La contrainte budgétaire pesant sur l'action de l'État étant particulièrement forte, il apparaît urgent à vos rapporteures que la stratégie nationale d'influence puisse formaliser des priorités stratégiques géographiques et thématiques claires, où porter les efforts.

En effet comme l'indique le Colonel Devigne dans la RDN « *Une stratégie informationnelle ne va pas sans une capacité de veille performante pour caractériser le risque avec précision, l'autorité suffisante pour choisir ses combats et ne pas éparpiller ses efforts, ainsi que la volonté de s'inscrire dans la durée sans obsession du résultat immédiat.* »

La définition de priorités claires doit permettre de mieux étudier les caractéristiques des populations concernées, d'affiner le ciblage et d'adapter les contenus en fonction.

● Le cap donné par la stratégie nationale d'influence doit également permettre de concentrer les moyens en fonction des objectifs fixés.

À cet égard, le tournant constitué par le désengagement des États-Unis dans le champ informationnel constitue à la fois un défi et une opportunité pour la France et l'Europe. En effet, le 15 mars dernier, l'administration américaine a pris la décision de cesser le financement des médias publics internationaux états-uniens pilotés par USAGM (*U.S. Agency for Global Media*) (*Radio Free Europe/ Radio Liberty, Voice of America, Radio Free Asia*, etc.). À cela s'ajoutent des coupes importantes dans le budget de l'USAID et dans le soutien aux journalistes locaux. Selon la directrice de France Médias Monde, auditionnée par vos rapporteures, il s'agit d'un événement de nature à modifier profondément, et durablement, le paysage audiovisuel mondial.

Vos rapporteures ont été alertées sur la nécessité de combler le « vide » laissé par les États-Unis, au risque de voir remplacer l'influence occidentale par celle de nos compétiteurs. Le risque est réel que cette décision crée un « appel d'air » pour les médias russes et chinois, qui profiteront inévitablement du retrait américain pour récupérer les fréquences laissées vacantes par les médias cessant d'émettre – situation déjà observée en 2023 lorsque la radio BBC Arabic a cessé d'émettre au Proche et Moyen-Orient et que ses fréquences ont été réattribuées à *Sputnik* en Syrie, en Irak et au Liban, selon les informations fournies par FMM.

Toujours selon FMM, il devient urgent d'apporter un appui politique et financier au niveau européen pour donner les moyens à l'audiovisuel public extérieur de renforcer son offre en langues étrangères, de soutenir les radios partenaires en Afrique et, en particulier, de récupérer les fréquences laissées vacantes par les médias de l'USAGM, de manière à éviter de libérer l'espace aux médias russes, chinois et turcs.

Aussi, FMM a-t-elle élaborée avec son partenaire allemand *Deutsche Welle* une proposition de plan de renforcement coordonné de leurs activités, nommé « Bouclier pour l'Information », afin de limiter les effets du désengagement américain sur le plan informationnel. Pour FMM, ce renforcement est chiffré à 25 millions d'euros supplémentaires par an. Selon les informations fournies à vos rapporteures, ces sommes resteraient modestes au regard du budget alloué jusqu'à présent aux médias publics internationaux américains, qui bénéficiaient de près d'un milliard d'euros (876 M€) pour opérer en plus de soixante langues, auprès de plus de 420 millions de téléspectateurs, d'auditeurs et d'internautes chaque semaine dans le monde.

À l'international, il convient également de poursuivre l'œuvre entreprise par Canal France International (CFI) afin d'agir contre la désinformation à l'étranger en formant des journalistes. CFI a été créée en 1989 par le ministère de la Coopération pour assurer la diffusion gratuite de programmes de télévision en Afrique francophone. En 2010, l'État lui confie un mandat unique : celui d'être une agence de soutien aux médias. CFI est la filiale à 100 % de France Médias Monde. L'agence développe et met en œuvre des projets d'aide publique au développement par les médias en accompagnant, dans plusieurs régions du monde (Afrique, monde arabe, Europe orientale, Asie du sud-est), les médias locaux ainsi que les acteurs de la société civile engagés pour une information pluraliste et démocratique. Son contrat d'objectifs 2024-2028 signé en juillet 2024 avec le Ministère de l'Europe et des Affaires étrangères fixe des objectifs sur quatre thématiques prioritaires : la lutte contre la désinformation, la défense de l'égalité femmes-hommes, la protection de l'environnement et la promotion de la démocratie et de l'engagement citoyen, en particulier de la jeunesse. 39 projets ont été menés par CFI en 2024, dont la moitié l'a été conjointement avec France Médias Monde. Un grand nombre de ces projets ont pour objectif principal de conforter les capacités de lutte contre la désinformation à travers, par exemple, les projets « *Désinfox Réseau* » ; « *Désinfox Côte d'Ivoire* » ; « *Désinfox jeunesse* » ; ou encore « *Radio Check Togo* ». Ils s'incarnent principalement à travers des actions de formation pour le renforcement des capacités des professionnels locaux, mais aussi des sociétés civiles, en matière de fact-checking par exemple.

Le MEAE finance par ailleurs l'accès au fil des dépêches AFP pour des médias africains (plutôt qu'ils ne republient des dépêches chinoises, qu'ils ont gratuitement).

Vos rapporteures appellent également à poursuivre le soutien aux journalistes en exil, notamment russes. RSF appelle, par exemple, la Commission européenne à inclure des recommandations aux États-membres sur la manière de faciliter, depuis leur entrée sur le territoire de l'UE jusqu'à la reprise de leur activité professionnelle, l'autonomisation des journalistes en exil qui sont des acteurs en puissance de la lutte contre les manipulations de l'information et la propagande issue de leur pays d'origine. Concernant l'accueil des journalistes étrangers, RSF collabore d'ailleurs avec CFI, notamment à travers le programme « Voix en exil ». Avec l'appui du MEAE, ce programme de soutien et d'accompagnement doit

permettre à une trentaine de journalistes en exil à Paris de se former pour poursuivre leur travail d'information, crucial tant pour leurs concitoyens que pour le reste du monde.

● Enfin, au-delà de la nécessité de combler le vide laissé par le désengagement américain, vos rapporteures estiment qu'il convient de renforcer les moyens de diffusion en langue russe.

c. La nécessité de mieux identifier les moyens alloués à cette nouvelle fonction dans une logique de transparence

En cohérence avec l'augmentation des moyens, vos rapporteures estiment nécessaire de mieux identifier les moyens financiers et humains alloués à la fonction stratégique influence.

Cet effort de transparence apparaît nécessaire pour que le Parlement puisse être à même de contrôler l'action du Gouvernement en la matière et vérifier que les moyens soient bien en adéquation avec les objectifs fixés.

Vos rapporteures préconisent donc que soit identifié un « patch influence », dans la loi de programmation militaire et dans la stratégie nationale d'influence, qui préciserait clairement les crédits et les effectifs alloués à l'opérationnalisation de la fonction stratégique, dont le suivi pourrait être assuré dans les documents budgétaires chaque année.

Cet effort de transparence est d'autant plus important, compte tenu de la réputation sulfureuse que peuvent avoir les opérations d'influence en démocratie.

Recommandation : Identifier un « patch influence » dans la loi de programmation militaire et dans la stratégie nationale d'influence, précisant clairement les crédits et les effectifs alloués à l'opérationnalisation de la fonction stratégique influence et dont le suivi pourrait être assuré dans les documents budgétaires chaque année.

d. … et de mieux mesurer l'efficacité des actions menées

● Dans une même logique de contrôle des dépenses publiques, il convient de mieux mesurer l'efficacité des actions menées en matière d'influence, voire d'envisager la création d'indicateurs de performance dédiés.

S'il est difficile de mesurer l'efficacité des effets produits – car il existe une gradation des effets entre l'absence de résultat et le changement de comportement ; objectif *in fine* des actions d'influence – il est en revanche possible de mesurer la performance, soit le volume d'utilisateurs touché par une action. Ce n'est pas un indicateur parfait mais cela permet une première évaluation des actions, même si les effets se mesurent en réalité sur le temps long et sont le résultat de la combinaison de plusieurs actions d'influence. Selon les personnes auditionnées, l'idée d'externalisation des capacités d'analyse et de mesure des effets, comme le

pratiquent les Britanniques et les Américains, représente une piste de réflexion qui offre une certaine agilité et des économies en termes RH.

● De plus, il semble crucial d'apporter une importance particulière à l'analyse du retour d'expérience pour identifier les méthodes et narratifs les plus efficaces.

En particulier, **vos rapporteures estiment nécessaire de tirer plus clairement pour le ministère des armées et des affaires étrangères les conséquences de l'échec sahélien, notamment dans le champ informationnel.**

C. AGIR EN AMONT POUR RÉDUIRE LES FACTEURS STRUCTURELS DE VULNÉRABILITÉ FACE AUX MANIPULATIONS DE L'INFORMATION EN ASSOCIANT LA SOCIÉTÉ CIVILE

L'existence d'acteurs spécialisés dans la défense de l'espace informationnel ne doit pas conduire à la déresponsabilisation du citoyen. Au contraire, il ressort des travaux de vos rapporteures que la société civile doit être placée en première ligne de la lutte contre les manipulations de l'information pour bâtir une politique publique réellement efficace.

L'efficacité de la politique menée dépend, en outre, de l'identification puis de la résorption des vulnérabilités préexistantes. Au-delà de s'attacher à renforcer l'immunité collective de la société française face aux manipulations de l'information, il convient de prendre en compte la guerre cognitive comme une composante majeure de la guerre de demain, sans pour autant négliger l'interconnexion entre les champs physiques et informationnels.

1. Renforcer l'immunité collective de la société française

L'analogie entre la désinformation et la propagation d'un virus est parlante pour prendre la mesure du phénomène auquel les démocraties doivent faire face. Ainsi, l'historien David Colon, n'hésite pas à employer le terme de « *pandémie informationnelle* ». Il encourage à prendre en compte le processus d'émission d'un « virus informationnel » et d'appliquer les méthodes de contrôle des pandémies à la désinformation, à l'image de la mesure des effets prévisibles de la propagation pour mieux l'enrayer. Le degré d'exposition du public est en effet clé pour déterminer la dangerosité d'une campagne informationnelle.

Aussi, vos rapporteures considèrent-elles qu'il convient d'abord d'objectiver les conséquences de stratégies de désinformation sur la société française pour mieux identifier ses vulnérabilités, afin d'être en mesure d'agir en amont pour les réduire. Cela suppose notamment de mieux prendre en compte les défis posés par les réseaux sociaux en matière de lutte contre la désinformation, notamment en période électorale, mais surtout de bâtir une politique visant à mieux associer la société civile.

a. Objectiver les conséquences des stratégies de désinformation sur la société française et identifier les vulnérabilités

● **Objectiver les conséquences des stratégies de désinformation sur la société française est essentiel afin de ne pas surestimer ni sous-estimer la menace, voire risquer d'amplifier l'effet déstabilisateur sur nos sociétés des stratégies menées par nos compétiteurs.** Il s'agit d'un préalable essentiel à l'élaboration d'une réponse efficace.

Si nos compétiteurs investissent des sommes importantes dans leurs campagnes informationnelles, il est logique de penser qu'ils y trouvent un intérêt. Toutefois, vos rapporteures ne peuvent se satisfaire de cette première intuition.

Il ressort des auditions menées par vos rapporteures qu'il existe un véritable déficit d'études scientifiques portant sur les effets tangibles de la désinformation sur la société française. Au-delà des études portant sur la circulation de l'information, il convient donc de s'attarder sur la réception de l'information, afin d'étudier la manière dont la circulation se transforme en adhésion puis en croyance ferme, voire en passage à l'action. Une des difficultés principales consiste à mesurer les conséquences de l'accumulation des récits et non d'un seul récit, qui, pris isolément, peut ne pas produire d'effets mais dont l'accumulation peut profondément contribuer à déstabiliser une société en y faisant régner le doute généralisé.

Certains travaux tentent d'identifier les facteurs de la perméabilité à la désinformation mais soulignent la nécessité d'encourager des travaux scientifiques plus complets en la matière. Dans une étude récente parue en novembre 2024, la Fondation Descartes [(1)], à travers son directeur de la recherche, Laurent Cordonier, auditionné par vos rapporteures, cherche à mieux comprendre les effets sur l'opinion publique française des guerres informationnelles liées aux conflits contemporains. L'étude démontre que plus les Français interrogés se montrent sensibles au récit russe, par exemple, plus ils ont tendance à l'être également aux récits du Hamas, malien et chinois, et moins ils ont tendance à l'être aux récits ukrainien, israélien, français et taïwanais. Par ailleurs, l'étude cherche à identifier les facteurs de sensibilité des Français aux différents récits testés. Davantage que les caractéristiques sociodémographiques ou politiques des individus, un facteur qui semble particulièrement influencer la sensibilité des Français aux différents récits est leur comportement d'information. La confiance que les Français ont, de manière générale, dans les médias ou les réseaux sociaux présente un effet symétrique sur leur sensibilité aux différents récits. Un autre enseignement de l'étude est qu'une majorité de la population (62,1 %) estime que les attaques informationnelles russes et chinoises qui ciblent la France représentent un danger pour le pays et sa démocratie. Il ressort de l'étude que les Français qui s'informent plus fréquemment que les autres sur l'actualité internationale via les réseaux sociaux, YouTube ou les

(1) Laurent Cordonier (2024). Pénétration en France des récits étrangers sur les conflits contemporains. Étude de la Fondation Descartes. (lien).

messageries instantanées sont en moyenne plus sensibles aux récits russe et chinois. Ce résultat laisse penser que les opérations d'ingérences informationnelles menées par ces deux pays dans l'univers numérique français produisent un certain effet sur les représentations des citoyens qui s'y informent régulièrement. Cependant, on constate également que la population française se montre dans l'ensemble très peu sensible aux récits russe et chinois, alors qu'elle l'est bien davantage aux récits de leurs adversaires directs (respectivement, l'Ukraine et Taïwan). Cela indique clairement que les manipulations de l'information russes et chinoises échouent (jusqu'ici, du moins) à faire basculer l'opinion publique française en faveur des récits qu'elles promeuvent sur la guerre en Ukraine et sur le statut de Taïwan. Ce n'est pas nécessairement pour autant que les opérations d'ingérences informationnelles étrangères demeurent sans effet sur la population française. Une de leurs conséquences possibles, qui est visiblement recherchée par les acteurs à l'origine de ces opérations, est de **polariser l'opinion publique sur des questions de société ou de politique intérieure.** Souvent, cela passe par le fait d'appuyer sur des fractures existantes, dans l'espoir de les aggraver. On ne sait cependant pas dans quelle mesure de telles opérations contribuent effectivement à polariser l'opinion publique française.

En conséquence, la Fondation Descartes partage le constat de la nécessité d'une meilleure évaluation de la nature et de l'ampleur des conséquences des ingérences informationnelles étrangères sur la population française. En effet, sans disposer d'une telle évaluation, qui fait aujourd'hui largement défaut, il est impossible de calibrer correctement la réponse des pouvoirs publics et des acteurs de l'information à ces opérations de manipulation. Sous-réagir exposerait le pays à un risque de déstabilisation. Surréagir, par exemple, en adoptant des mesures restreignant trop sévèrement la liberté d'expression en ligne ou en invisibilisant totalement dans les médias certains points de vue sur l'actualité internationale, reviendrait à abîmer la vie démocratique en cherchant à la protéger.

Recommandation : Encourager et soutenir les travaux de recherche scientifique visant à objectiver les conséquences des ingérences informationnelles étrangères sur la société française afin de ne pas surestimer ni sous-estimer la menace, voire risquer d'amplifier l'effet déstabilisateur sur nos sociétés des stratégies menées par nos compétiteurs.

● **Il convient, en outre, de mieux appréhender les ressorts individuels et collectifs de la perméabilité à la désinformation.** Il ne s'agit ici aucunement de porter un jugement de valeur sur une partie de la population présentée comme plus vulnérable, tant la désinformation affecte toutes les composantes de la société et devient de plus en plus pernicieuse à identifier à mesure qu'elle devient difficile à détecter même pour un œil averti, néanmoins l'identification des vulnérabilités doit permettre de construire une politique publique à même de traiter les causes structurelles de la sensibilité à la désinformation.

Le rapport du CAPS et de l'IRSEM de 2018 précité mettait ainsi en lumière plusieurs facteurs d'explication qui demeurent pertinents, au premier rangs desquels l'existence de biais cognitifs individuels et collectifs, mais surtout la crise de confiance dans les institutions.

La mise en évidence des causes structurelles de la sensibilité à la désinformation démontre à quel point la réponse aux manipulations de l'information doit constituer une politique publique d'ensemble, dont les solutions ne résident pas exclusivement dans le champ informationnel. En effet, selon Grégoire Darcy (1), chercheur en sciences sociales cognitives, « *la lutte contre la désinformation se focalise souvent sur son atténuation immédiate, la traitant comme un fléau isolé, alors qu'elle est le symptôme de dysfonctionnements profonds dans nos écosystèmes sociaux et institutionnels*. » Or, chercher à traiter les symptômes de la désinformation sans s'attaquer à ses causes structurelles peut s'avérer vain : « *la diffusion, la force de persuasion et l'efficacité de la désinformation reposent principalement sur l'épidémie de solitude, la défiance grandissante envers les institutions et les médias, ainsi que sur l'intensification de la polarisation, des tensions entre groupes et de la précarité économique. Il est en conséquence impératif de compléter les réponses curatives spécifiques à court et moyen terme actuellement déployées par des politiques de fond, capables de traiter directement le mal à la racine.* »

b. Agir en amont pour réduire les facteurs structurels de vulnérabilités face à la désinformation

i. À court terme : poursuivre les actions de *pre-bunking* et de *debunking* afin de limiter l'effet des narratifs adverses

● Malgré les limites identifiées aux actions de riposte, il convient à court terme de ne pas laisser le champ libre aux acteurs hostiles et de continuer à porter la contradiction aux compétiteurs dans le champ informationnel.

Pour ce faire, plusieurs méthodes peuvent être utilisées notamment le *debunking (démasquer,démystifier*) et le *pre-bunking (réfutation par anticipation)*.

Toutefois, la désinformation tend à se propager plus rapidement qu'elle ne peut être réfutée. C'est pourquoi, moins connue que le *debunking* la méthode du *pre-bunking* ou de réfutation par anticipation, vise à agir en amont de la diffusion d'une fausse information en vue d'en limiter les effets. Selon la définition apportée dans le rapport des États généraux de l'information, le *pre-bunking* constitue une technique préventive de lutte contre la manipulation de l'information consistant à créer des « anticorps mentaux » en aidant le public à identifier et à réfuter par anticipation des récits faux et trompeurs de sorte d'« immuniser » la société contre

---

(1) Grégoire Darcy. ENS-PSL, Département d'Études Cognitives. Enseigne les sciences cognitives appliquées aux champs culturels et informationnels à l'EMSST – École Militaire - lien ; et Darcy, G. et al. 2025. " Lutter Contre La Désinformation : Penser Autrement L'action Publique À L'aune Des Sciences Cognitives. " OSF Preprints. May 28. doi:10.31219/osf.io/fu9cz_vl.

les effets de campagnes de désinformation. À la différence du *debunking*, le *pre-bunking* ne repose pas sur l'énonciation de ce qui est vrai ou faux, mais sur l'exposition préventive aux principales techniques de manipulation auxquelles le public peut être exposé – comme le recours aux émotions, l'usurpation d'identité, le *trolling*, la décontextualisation, etc.

Les dispositifs de *pre-bunking* prennent la forme de campagnes d'information ou de jeux sérieux, à l'image de ceux conçus par l'équipe du psychologue social Sander van Der Linden pour le compte de l'OMS, du Gouvernement britannique ou du Département d'État des États-Unis (*goviralgame.com ; hgetbadnews.com ; harmonysquare.game*). Une étude de Roozenbeek et al. (2022) a ainsi démontré que de courtes vidéos animées présentant des tactiques de manipulation amélioraient significativement la capacité des utilisateurs à distinguer les *fake news* des informations véridiques (1).

Toutefois, il convient d'apporter une attention particulière à l'enjeu relatif à la diffusion des analyses de *prebunk* et de *debunk* pour garantir leur efficacité. Si VIGINUM opère un travail de veille majeur, l'opérateur ne dispose pas de capacités de diffusion pour « *debunker* ». Il s'agit donc de s'appuyer sur les cellules de *fact-checking* existantes dans les médias. Ce travail est notamment opéré à travers des émissions dédiées comme « Les Dessous de l'infox » ou « L'Atelier des médias » sur RFI, ou encore « Les Observateurs » sur France 24.

Toutefois, il convient de prendre en compte les risques associés et les craintes parfois légitimes autour du *fact-checking* en garantissant un réel professionnalisme des médias en la matière. L'accusation de propagande et le recours au concept de désinformation peut en effet facilement être perçu comme une façon de clore un débat, comme le pointe la Fondation Jean Jaurès dont une récente étude (2).

C'est pourquoi, il semble important de mettre en lumière les systèmes et les stratégies globales de désinformation, en s'attachant à ne pas traiter uniquement des détournements ou des fausses informations ponctuelles prises isolément. À titre d'exemple, le *Propaganda Monitor*, lancé par RSF s'inscrit dans cette démarche.

Enfin, il convient d'étudier la manière dont l'IA générative peut aider à prévenir la propagation de contenus malveillants et surtout ses effets néfastes, à l'image des tests de dépistage de la susceptibilité à la désinformation ou des outils pour concevoir des contre narratifs testés scientifiquement pour leur efficacité. Comme l'indique David Colon dans un article de la RDN (3) , des chercheurs ont ainsi testé avec succès à l'été 2024 le *prebunking* assisté par IA générative pour

---

(1) Ibid.

(2) Guillaume Caline, Laurence Vardaxoglou, Regard des Français sur la lutte contre la désinformation, Fondation Jean Jaurès, novembre 2024. (lien).

(3) Colon, D. (2025). La « défense psychologique » face aux manipulations de l'information. Revue Défense Nationale, 876(1), 57-65. https://doi.org/10.3917/rdna.876.0057.

réduire à la croyance dans des fausses informations relatives aux élections et augmenter la confiance des électeurs dans l'intégrité du vote [1].

Recommandation : À court terme, encourager les actions de *debunking* et surtout de *prebunking*, prises comme des outils parmi d'autre dans la lutte contre les manipulations de l'information, tout en demeurant conscients de leurs limites.

ii. À moyen et long termes : renforcer l'éducation aux médias et à l'esprit critique

● **Si l'éducation aux médias et à l'esprit critique semble devenue un « poncif » des instruments de lutte contre la désinformation, sa promotion n'en demeure pas moins primordiale.** Néanmoins, le choix de la méthode retenue doit se fonder sur une approche scientifique pour éviter tout effet pervers. Contrairement aux idées reçues, elle ne doit pas s'adresser exclusivement à la jeunesse mais à l'ensemble des classes d'âge pour bâtir une véritable résistance collective. Les actions de sensibilisation menées doivent permettre de mieux appréhender la manière dont fonctionnent les outils de désinformation et les algorithmes, en s'appuyant au besoin sur des méthodes innovantes. **Il ne s'agit pas d'enseigner ni de dire quoi penser, mais bien d'apprendre à le faire en conscience et avec les bons outils.**

● De nombreux rapports appellent à faire de l'éducation une priorité. Le rapport Bronner [2] appelait déjà en 2022 à faire du développement de l'esprit critique et de l'éducation aux médias une « grande cause nationale ».

Cette ambition s'est depuis concrétisée au travers plusieurs projets, structurels ou ponctuels, visant à intégrer l'éducation aux médias et à l'information (EMI) dans la formation de l'ensemble des élèves. Entre 2024 et 2025, 345 749 élèves ont bénéficié d'une action d'EMI [3]. Cet effort doit désormais être approfondi pour intégrer la population dans son ensemble.

Toutefois, l'EMI ne dispose pas d'un nombre d'heures dédiées dans l'emploi du temps des élèves. Transversale, l'EMI se déploie tout au long de la scolarité, du cycle 2 au lycée, en lien avec les différents programmes d'enseignement (dans le cadre des cours ou dans les actions éducatives). L'EMI est notamment prégnante dans les programmes d'EMC dont la quotité horaire hebdomadaire (1/2h) demeure extrêmement limitée et inégalement dispensée.

● **Des progrès récents ont été réalisés et doivent être poursuivis mais surtout mieux identifiés.**

---

(1) LINEGAR Mitchell, SINCLAIR Betsy, VAN DER LINDEN S. et ALVAREZ R. Michael, « Prebunking Elections Rumors:Artificial Intelligence Assisted Interventions Increase Confidence in American Elections », Preprint, 24 octobre 2024.

(2) « Les Lumières à l'ère numérique », rapport de la commission, présidée par Gérard Bronner, janvier 2022. (lien).

(3) D'après le site ADAGE, plateforme numérique de l'Éducation nationale dédiée à la généralisation de l'éducation artistique et culturelle.

Conformément à la circulaire du 24 janvier 2022 sur la généralisation de l'éducation aux médias et à l'information, une place croissante est accordée à l'EMI dans les programmes scolaires à tous les niveaux. Cela implique à la fois la création de nouveaux enseignements proposés aux élèves mais également de nouvelles formations à destination des professeurs. La Direction Générale de l'Enseignement Scolaire (DGSCO), en charge de l'élaboration des programmes scolaires, travaille en étroite collaboration avec le Centre pour l'Éducation aux Médias et à l'Information (CLEMI), un des organismes du Réseau Canopé [(1)], spécialisé dans la production de contenus, l'organisation de concours nationaux de médias scolaires et d'exercices ludiques afin de former et de sensibiliser les enseignants et les élèves à l'EMI. Le CLEMI peut s'appuyer sur un vaste réseau de coordinateurs académiques et de référents académiques EMI, qui sont en charge d'une cellule EMI au sein de chaque rectorat.

D'une part, depuis la rentrée 2024, de nouveaux programmes d'Éducation Morale et Civique accordant une part plus importante à l'EMI sont progressivement entrés en vigueur. D'ici trois ans, l'ensemble des niveaux bénéficieront de ces nouveaux enseignements spécifiques.

D'autre part, un effort devrait également être réalisé en direction de la formation des enseignants au travers de plusieurs programmes nationaux de formation (PNF) en matière d'EMI. Le premier, sous forme de webinaires consacrés à la lutte contre les manipulations de l'information, devrait être développé dès juin 2025. Le second, à destination des enseignants et des cadres de l'éducation nationale, devrait porter sur la thématique « *IA, numérique et défense* » et est prévu pour la rentrée 2025.

Cette importance accordée à l'EMI devrait être réaffirmée prochainement dans un projet de loi visant à reprendre une partie des recommandations des États Généraux de l'Information. Vos rapporteures seront particulièrement vigilantes à ce que le projet de loi accorde effectivement une place renforcée à l'EMI.

Enfin, selon les informations fournies à vos rapporteures, à l'échelle interministérielle, une feuille de route est en cours de finalisation entre la DGESCO et VIGINUM et devrait structurer leur coopération pour la période 2025-2026. Elle prévoit la mise en place d'un certain nombre de mesures, telles que la multiplication de séminaires de formation à destination de la communauté éducative, la production de ressources pédagogiques et le développement de collaborations avec le réseau des écoles françaises à l'étranger. Cette feuille de route vient entériner une coopération déjà très active, avec des projets tels que le podcast « *Clara et Raphaël » ;* un format de contenu ludique conçu pour susciter l'intérêt des jeunes tout en les informant sur différentes formes de désinformation en ligne. Le CLEMI travaille également avec le COMCYBER avec qui il a produit l'exercice « Passe

(1) « Sous la tutelle du ministère de l'Éducation nationale, Réseau Canopé est l'opérateur de la formation tout au long de la vie des enseignants et des acteurs de l'éducation. ». (lien).

ton hack d'abord » (1) , et avec le ministère des affaires étrangères dans le cadre de la feuille de route « médias et développement 2023-2027 » de la direction générale de la mondialisation. Enfin, il développe le Réseau Francophone d'Éducation aux Médias et à l'Information (REFEMI) créé en octobre 2024 lors du 19e Sommet de la Francophonie.

La coopération avec les médias semble solide et fructueuse et le CLEMI souligne la bonne volonté des médias français avec lesquels il a mis en place un certain nombre d'initiatives. Ainsi, le CLEMI organise avec les médias son évènement phare, la « **Semaine de la presse »**, auquel environ quatre millions d'élèves participent chaque année depuis 2010.

L'ensemble de ces projets consiste à informer les élèves au travers d'activités ludiques, les mettre en garde et les former en les faisant participer à des jeux d'enquête et d'analyse ou bien des concours de production médiatique. Cependant le CLEMI reste prudent vis-à-vis des « *serious games* », développés par des chercheurs de l'université de Cambridge lorsque ceux-ci consistent en la fabrication de fausses informations par les élèves eux-mêmes. Si le chercheur David Colon souligne l'intérêt de cette méthode en ce qu'elle permettrait la « vaccination mentale » des plus jeunes par une sorte d'inoculation à la désinformation, le CLEMI préfère mettre l'accent sur les fondamentaux de l'EMI et un rapport sain à l'information pour les élèves.

● **Un des défis principaux rencontré par CLEMI est de susciter l'intérêt des jeunes**. C'est dans ce but que, de manière ponctuelle, il fait appel à des « influenceurs de confiance » afin de relayer efficacement leurs contenus et opérations de sensibilisation sur les réseaux sociaux et les plateformes de streaming en ligne comme Twitch (2). Pour autant, le recours à des influenceurs afin de toucher le plus efficacement possible les jeunes n'est à l'heure actuelle pas pleinement exploité par l'Éducation nationale. En effet, malgré des initiatives telles que la formation proposée par l'UNESCO à des influenceurs en matière d'éducation aux médias d'éthique et de responsabilité (3), la plupart des influenceurs restent des partenaires jugés encore trop peu fiables pour que les institutions les sollicitent pleinement.

Vos rapporteures considèrent que le recours aux méthodes innovantes pourrait encore être amplifié. Pour maximiser l'impact de l'EMI, il est important de généraliser son accès à tous les élèves et diversifier les méthodes pédagogiques pour éviter une approche perçue comme moralisante. L'exemple de l'opération « Cactus » menée auprès des élèves de collège et de lycée des académies volontaires constitue un exemple intéressant qui pourrait être étendu à la lutte contre les manipulations de l'information. Le Parquet de Paris (section de lutte contre la cybercriminalité – J3) associé à un collectif d'acteur a ainsi mené une opération de

(1) Site du ministère des armées. (lien).

(2)Site du CLEMI « Les Invités du CLEMI : Produire de l'info en live sur Twitch avec les élèves ». (lien).

(3) Projet conjoint entre l'UNESCO et le *Knight Center for Journalism* porté par Adeline Hulin. *(lien).*

sensibilisation basée sur une simulation d'hameçonnage, première menace cyber en France. Après une phase d'expérimentation réussie en mai 2025, l'opération Cactus est aujourd'hui élargie à l'ensemble des académies françaises. Les élèves ont ainsi reçu un message, *via* leur espace numérique de travail ou le logiciel de vie scolaire (PRONOTE), les incitant à cliquer sur un lien pour se procurer gratuitement des *« jeux crackés et des cheats gratuits »*. L'objectif de cette action est principalement de sensibiliser et responsabiliser les jeunes en marquant leur esprit avec des messages forts, au travers d'une communication des autorités en charge des sujets de cybersécurité.

● Toutefois, **pour massifier l'EMI, il faut doter le CLEMI des moyens de ses ambitions**. Le CLEMI compte actuellement vingt-quatre ETP (1) pour remplir sa mission et dispose d'un budget de fonctionnement de 597 870 €. Une augmentation de moyens lui permettrait d'intensifier son action sur le territoire national, en augmentant la production de contenus informatifs par exemple, mais également à l'étranger. En effet il est sollicité par des pays comme le Brésil, le Canada mais également l'UNESCO pour apporter son aide dans la création de structures analogues au CLEMI. La Cour des comptes a d'ailleurs déclaré que le Réseau Canopé, tutelle du CLEMI « *doit pouvoir se positionner sur l'avenir du CLÉMI afin qu'il puisse véhiculer largement la politique d'éducation aux médias et à l'information voulue par l'État, notamment en disposant de moyens propres et d'un budget fléché* » (2) dans son rapport du 3 octobre 2024.

Recommandation : Investir de manière croissante dans la construction de la résilience de la Nation à travers le renforcement de l'éducation aux médias et à l'esprit critique, en cohérence avec l'accroissement de l'investissement consenti en faveur des capacités de détection et de caractérisation de la menace informationnelle.

● **Au-delà de la question des moyens, deux lacunes principales limitent pour l'instant la pleine efficacité des actions menées en faveur de l'éducation aux médias et à l'esprit critique.**

La première fragilité du dispositif réside dans **le manque d'évaluation -** une lacune qui a été mise en avant par les chercheurs auditionnés, notamment M. Laurent Cordonier de la Fondation Descartes.

D'une part, il convient **d'évaluer scientifiquement les méthodes d'EMI pour en connaître les effets produits sur le public visé et ainsi déterminer quelles méthodes s'avèrent réellement efficaces, avant de les généraliser.** Cela permettrait également de remédier à une trop grande multiplication des initiatives au détriment de la cohérence d'ensemble du dispositif d'éducation à l'EMI. Cela permettrait également d'éviter les éventuels effets pervers liés à une trop forte exposition à la désinformation et des mises en garde trop fréquentes qui pourraient

(1) Plus précisément, une masse salariale :de 1 647 560 € (24,2 ETP) ; dont actuellement 21,2 ETP, une enseignante détachée PALD, et deux apprentis.

(2) Cour des comptes, Le réseau Canopé, octobre 2024. (lien). (p.42)

à terme conduire à la perte complète de confiance en l'information de la part des jeunes.

D'autre part, il faut évaluer l'efficacité des dispositifs déjà mis en place. Si une étude a déjà été menée en 2024 (1) et montre que l'EMI a déjà permis de former des élèves à de bonnes pratiques vis-à-vis de l'information, et que ces derniers disposent désormais de bons réflexes (diversification des sources, précaution face à des informations en ligne), il apparaît indispensable de systématiser et d'approfondir ces études d'impact, tant pour gagner en efficacité que se prémunir de potentiels effets pervers de mauvaises méthodes. C'est d'ailleurs pour éviter ce dernier point qu'il est fondamental de porter un discours positif et constructif, de signaler les menaces tout en valorisant les forces de notre environnement informationnel.

Enfin, pour être pertinentes, **les mesures de construction de la résilience doivent concerner l'ensemble de la société, en complément des actions à destination de la jeunesse**. L'EMI doit devenir « l'affaire de tous ». En dépit de quelques mesures, telles que les fiches sur parentalité numérique produites par le CLEMI (2) et des campagnes ponctuelles de sensibilisation des cadres dirigeants de l'État et du monde de l'entreprise à l'occasion des cycles de séminaire de l'Institut des hautes études de défense nationale (IHEDN), de l'Institut des hautes études du ministère de l'Intérieur (IHEMI), des écoles et universités et auprès du Mouvement des Entreprises de France (MEDEF) entreprises par VIGINUM, **la sensibilisation de la société dans son ensemble demeure un angle mort de l'EMI.**

Pour sensibiliser plus largement l'ensemble de la population, plusieurs pistes mériteraient d'être étudiées. Tout d'abord, vos rapporteures considèrent que le SGDSN gagerait à intégrer un volet sur l'EMI au guide de résilience devant être distribué aux Français en 2025. Par ailleurs, il conviendrait d'étudier la possibilité de mettre à profit la journée nationale de la résilience, organisée localement le 13 octobre de chaque année, pour mener des actions de sensibilisation à destination de la population toute entière. De la même manière, la journée défense et citoyenneté (JDC), qui fait actuellement l'objet d'une refonte, pourrait également intégrer une séquence consacrée au risque informationnel.

Recommandation : Intégrer un volet sur l'EMI au guide de résilience devant être distribué à aux Français en 2025 et étudier l'opportunité de mettre à profit la journée nationale de la résilience et la journée de défense et de citoyenneté pour mener des actions de sensibilisation à destination de la population toute entière.

(1) Il s'agit de l'étude CLEMI'Sup (2024) « Les pratiques informationnelles des adolescents 2023, désinformation & vérification de l'information » de Sophie Jehel (menée sur 1.284 lycéens en filière professionnelle). (lien).

(2) Site Internet du CLEMI « Parentalité et bien-être numérique ». (lien).

c. Mieux prendre en compte les défis posés par les réseaux sociaux et les médias en matière de lutte contre la désinformation

Bien qu'ils dépassent le champ de la commission de la défense, vos rapporteures ont souhaité aborder les défis posés par les médias et les réseaux sociaux en matière de lutte contre la désinformation. Les grandes plateformes constituent en effet un lieu privilégié de relais pour les manœuvres informationnelles. Tik Tok avait d'ailleurs été qualifié « d'arme informationnelle [(1)] » par le CEMA lors d'une audition de la commission.

Si le Règlement sur les services numériques ou *Digital Services Act* (DSA) semble constituer un cadre juridique adapté, son application pleine et entière demeure un véritable enjeu, tandis que le financement des médias traditionnels doit constituer un sujet de préoccupation.

Les périodes électorales constituent par ailleurs une vraie vulnérabilité. Il convient de se prémunir de la réalisation d'un scénario « à la roumaine ».

i. L'enjeu de l'application du cadre juridique existant

Les personnes auditionnées ont insisté sur la nécessité de poursuivre la responsabilisation des plateformes et de mieux faire appliquer le cadre juridique en vigueur.

● **Actuellement, la réponse de l'UE aux manipulations l'information repose essentiellement sur l'application du DSA,** qui s'appuie sur une approche de réduction des risques systémiques par les plus grandes plateformes numériques. Ce cadre juridique doit être pleinement mobilisé pour faire respecter leurs obligations aux plateformes, en particulier en matière de lutte contre la désinformation et contre la haine en ligne. Lorsque ces obligations ne sont pas respectées, des sanctions doivent être prises à leur encontre, conformément à la législation européenne. Il ressort des auditions menées que le principal obstacle réside dans la lenteur des enquêtes ouvertes par la Commission européenne, notamment s'agissant de la plateforme X, qui s'accommode mal avec la vitesse de propagation des manœuvres informationnelles ou la temporalité d'élections.

Par ailleurs, il convient de relever que les capacités d'action de la France pour lutter contre les manipulations de l'information sont, en réalité, limitées précisément du fait du DSA qui confie à la Commission européenne la compétence pour réguler les principales plateformes qui y sont assujetties. Seules les plateformes établies en France, et qui ont moins de 45 millions d'utilisateurs actifs mensuels dans l'UE, relèvent de la juridiction des autorités françaises. L'échelon européen semble néanmoins le niveau adéquat pour opérer avec les grandes plateformes.

---

(1) Général Thierry Burkhard, chef d'état-major des armées, Commission de la défense, lors de son audition à huis clos, sur la contribution des armées à une nouvelle politique africaine de la France, le 31 janvier 2024.

À cet égard, vos rapporteures saluent la position de fermeté adoptée par le ministre des affaires étrangères, Jean-Noël Barrot, à l'égard des plateformes. Le ministre a ainsi encouragé la Commission à faire usage des pouvoirs que lui confèrent le DSA et d'être beaucoup plus rapide dans la mise en œuvre. Dans une récente interview le ministre Jean-Noël Barrot incitait l'Union européenne à faire aboutir les enquêtes contre Tik Tok et X et à renforcer les sanctions en cas d'ingérences étrangères notamment dans les processus électoraux comme en Roumanie, allant jusqu'à évoquer la possibilité pour la France de se protéger elle-même en cas de défaillance de la Commission européenne sur ce sujet.

● **Surtout, selon VIGINUM, la coopération avec les plateformes demeure un axe de progressi (1) on en matière d'identification et d'entraves.** VIGINUM suggère ainsi d'imposer aux plateformes de partager les informations dans le cadre de la lutte contre les ingérences numériques étrangères, en l'absence de réponse, des sanctions pourraient ainsi être établies.

ii. Redoubler de vigilance en période électorale

Vos rapporteures ont été particulièrement alertées au sujet des menaces entourant les élections. **Elles estiment qu'il convient à tout prix d'éviter un scénario « à la roumaine » en France et qu'il convient de renforcer le soutien à nos partenaires européens en la matière.**

● Selon les informations fournies à vos rapporteures, l'ingérence électorale constitue l'utilisation par une puissance étrangère de moyens clandestins, déceptifs ou coercitifs visant à altérer la tenue ou le résultat d'une élection dans un pays cible. Les exemples récents en Europe illustrent l'acuité de cette menace, qui est difficile à appréhender et à prévenir, car elle peut prendre des formes diverses, parfois simultanément.

Une puissance étrangère peut en effet vouloir s'ingérer dans un processus électoral pour deux types d'objectifs principaux :

– mettre en difficulté le gouvernement du pays cible ou saper la confiance de sa population dans sa démocratie et ses institutions, en entachant la crédibilité de l'élection ;

– favoriser la victoire ou la représentation d'individus, de partis ou d'idées politiques compatibles avec les objectifs de la puissance étrangère, en portant atteinte à l'intégrité du résultat électoral.

● Comme l'a révélé M. Marc-Antoine Brillant, chef de VIGINUM, « *depuis le milieu des années 2010, les manipulations de l'information impliquant des acteurs étrangers n'ont épargné aucun rendez-vous électoral ou référendaire*

(1) (lien).

majeur [(1)]».

Après la Géorgie et la Moldavie, la Roumanie est le troisième pays européen touché par des manipulations d'ampleur en contexte électoral en fin d'année 2024. Le 6 décembre 2024, la Cour constitutionnelle roumaine a ainsi pris la décision d'annuler « *l'ensemble du processus électoral relatif à l'élection du président de la Roumanie* », et a justifié cette décision en dénonçant de « *multiples irrégularités et violations de la législation électorale qui ont faussé le caractère libre et équitable du vote* », pointant notamment des infractions à la loi électorale et plus particulièrement en termes de transparence du financement de campagne. La Commission européenne a, quant à elle, ouvert une procédure formelle à l'encontre de TikTok dans le cadre du DSA.

Comme l'indique VIGINUM, premier scrutin démocratique majeur en Europe à avoir fait l'objet d'une décision d'annulation des résultats pour des soupçons d'ingérences étrangères, « *l'élection présidentielle roumaine de novembre 2024 marque un tournant dans la prise en compte de l'impact des manipulations de l'information sur les réseaux sociaux* ». Contrairement aux précédents « *L'élection présidentielle roumaine semble avoir été la cible d'une campagne numérique plus sophistiquée dans sa conception, centrée sur la manipulation de l'algorithme d'une plateforme particulièrement populaire en Roumanie, TikTok, et impliquant des écosystèmes de comptes prépositionnés ainsi que le recrutement d'influenceurs.* » « *Cette croissance fulgurante de la visibilité du candidat sur la plateforme semble avoir été obtenue grâce à une campagne d'astroturfing* [(2)] *sophistiquée, consistant en une manipulation coordonnée de l'algorithme de recommandation, via la publication massive de vidéos et de commentaires comportant certains hashtags et mots-clés. En effet, cette campagne a reposé, d'une part, sur l'action coordonnée de réseaux de comptes, et d'autre part, sur l'instrumentalisation de la popularité d'influenceurs rémunérés de manière dissimulée.* » [(3)]

Le service tire deux conclusions principales de l'analyse de cette campagne : d'une part, « *la relative facilité avec laquelle il est aujourd'hui possible d'imposer aux utilisateurs la visibilité d'un sujet sur un réseau social tel que TikTok, sans que le dispositif utilisé ne soit d'emblée modéré ou considéré comme inauthentique par la plateforme* », et d'autre part, « *le rôle et la vulnérabilité des influenceurs, exposés à un risque croissant d'instrumentalisation de la part d'acteurs malveillants utilisant des approches dissimulées* ». Et de conclure, que l'un des principaux préjudices causés par cette campagne de manipulation a été d'altérer la confiance des électeurs dans la fiabilité des processus électoraux.

---

(1) Rapport de la commission d'enquête concernant l'organisation des élections en France, Assemblée nationale, 28 mai 2025.

(2) Mode opératoire consistant à conférer de la visibilité à un sujet en faisant croire qu'il est un phénomène de masse alors même qu'il émane de la coordination de quelques comptes seulement qui produisent un volume important de publications sur un même sujet.

(3) Manipulation d'algorithmes et instrumentalisation d'influenceurs. Enseignements de l'élection présidentielle en Roumanie et risques pour la France, VIGINUM, février 2025.

En effet, il semble légitime de se demander si l'annulation de l'élection en Roumanie ne bénéficie pas, *in fine* aux acteurs à l'origine de cette potentielle opération d'ingérence, alimentant le discours sur la censure d'une partie des opinions politiques de la population. **C'est pourquoi vos rapporteures considèrent qu'il convient au maximum d'agir en amont, notamment par des actions d'éducation sur le long terme, décrites *supra*.**

La reproduction d'un tel mode opératoire en France ne semble pas exclue : « *il est donc légitime d'estimer qu'il existe un risque de transposition de ces modes opératoires dans le débat public numérique francophone afin de viser une audience française*. » En conséquence, VIGINUM adresse une alerte aux créateurs de contenus et influenceurs présents sur les réseaux sociaux sur le risque d'instrumentalisation dont ils pourraient faire l'objet de la part d'acteurs étrangers malveillants se dissimulant derrière des structures d'intermédiation commerciale.

Dans son rapport sur l'opération Storm-1516, VIGINUM fait d'ailleurs état d'une menace importante sur les processus électoraux y compris français. Le mode opératoire Storm-1516 a ainsi été employé « *pour cibler les élections européennes de juin 2024, les élections législatives anticipées françaises de juillet 2024, l'élection présidentielle américaine de novembre 2024, et les élections fédérales allemandes de février 2025. VIGINUM a ainsi été en mesure d'identifier au moins 20 opérations informationnelles visant ces différents scrutins. Celles-ci avaient pour objectif apparent de dénigrer un candidat à des élections nationales, de soutenir des candidats et des partis favorables aux intérêts du gouvernement russe et au positionnement « antisystème », ou encore de remettre en cause l'intégrité du scrutin*. » Ces manœuvres sont même allées jusqu'à la création d'un faux site électoral proposant de rémunérer des électeurs dans la volonté d'entacher la réputation du parti présidentiel : « *VIGINUM estime avec un niveau de confiance élevé que les opérateurs du réseau CopyCop, qui participent directement aux opérations de Storm-1516, ont enregistré dès le 19 juin 2024 le nom de domaine ensemble-24.fr, qui typosquattait le site officiel de la coalition « Ensemble » (ensemble-2024.fr) et usurpait son identité graphique. Le faux site affirmait que la coalition proposait aux électeurs de recevoir une « prime Macron » d'une valeur de 100 euros en échange de leur voix* [(1)]. »

● Face à ce constat, vos rapporteures considèrent qu'il convient de se prémunir de la réalisation de tout scenario de ce type, même si elles ne souhaitent pas dupliquer les travaux réalisés par la commission d'enquête de l'Assemblée nationale sur l'organisation des élections en France.

(1) Analyse du mode opératoire informationnel russe : Storm1516, VIGINUM, mai 2025.

Si le cadre juridique régissant la lutte contre les manipulations de l'information semble déjà relativement complet, un des enjeux principaux réside dans la temporalité très rapide de l'élection et la nécessité d'agir en amont afin d'éviter d'avoir recours à des mesures comme l'annulation des résultats a posteriori.

Vos rapporteures ont été alertées par les personnes auditionnées sur la nécessité de renforcer la réponse mise en place et la coordination des services de l'État en période électorale. Si la réponse semble plus aboutie dans le cadre des élections présidentielles, elle apparaît plus lacunaire lors des autres élections.

Les personnes auditionnées ont notamment indiqué que le rôle de VIGINUM en période électorale mériterait d'être clarifié. Si le service peut détecter une tentative d'ingérence numérique étrangère et le cas échéant en alerter les parties prenantes et autorités compétentes, VIGINUM ne dispose pas de la légitimité pour décider de rendre public une information qui pourrait potentiellement influencer le résultat du scrutin.

VIGINUM est en effet chargé de lutter contre les ingérences numériques étrangères. Découle de ce mandat la faculté d'analyser le contexte informationnel en période électorale et de fournir les informations utiles aux autorités chargées de contrôler le bon déroulement des élections (CNCCEP et ARCOM notamment). En effet, dans le cadre des élections présidentielles, il est prévu qu'une commission *ad hoc* se mette en place : la Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle (CNCCEP), présidée par le vice-président du Conseil d'État. La Commission exerce ses missions en relation avec d'autres institutions chargées de veiller au bon déroulement de l'élection : le Conseil constitutionnel, l'ARCOM, la CNIL, la Commission nationale des comptes de campagne et des financements politiques (CNCCFP), la Commission des sondages ou encore le Ministère de l'Intérieur. Au regard de son champ de compétence, l'on pourrait considérer que la CNCCEP serait la plus à même de rendre public avant même la tenue d'une élection, d'éventuelles anomalies détectées visant à influencer le résultat des élections éventuellement signalées par VIGINUM et de les transmettre au Conseil constitutionnel, juge de la régularité de l'élection présidentielle, dont il proclame les résultats. **En revanche, s'agissant des autres élections, il n'existe pas de commission comparable.** Le cas échéant, il n'existe pas actuellement d'organisme qui bénéficierait d'une légitimité suffisante et d'une objectivité reconnue pour prendre la décision de rendre public les éléments caractéristiques d'une tentative d'ingérence numérique étrangère. Deux modèles pourraient être envisagés, d'une part, la création d'une commission sur le modèle de la CNCCEP pour tout type d'élection, ou bien de confier cette mission à l'ARCOM, du fait de sa compétence dans le cadre du DSA. **Vos rapporteures seraient favorables à ce qu'une réflexion soit lancée, afin de déterminer s'il convient de compléter le droit existant ou a minima d'instaurer une coopération formalisée entre VIGINUM et la CNCCEP, dans la perspective des prochaines élections présidentielles.**

Recommandation : lancer une réflexion afin de déterminer s'il convient de compléter le droit existant ou a minima d'instaurer une coopération formalisée entre le VIGINUM et la CNCCEP, dans la perspective des prochaines élections présidentielles.

Cadre juridique relatif à la lutte contre les manipulations de l'information en période électorale

Sur le plan répressif, le code électoral sanctionne la diffusion de fausses informations visant à détourner les suffrages ou dissuader un ou plusieurs électeurs de voter (article L. 97 du code électoral).

Cet arsenal pénal a été complété par la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information qui a créé des outils spécifiques pour faire cesser rapidement la diffusion de fausses nouvelles, notamment en période électorale. Une procédure de référé « anti fake news » devant le juge judiciaire a notamment été mise en place, visant à faire cesser toute diffusion de fausses informations durant les trois mois précédant un scrutin national (article L. 163-2 du code électoral). Une disposition spécifique est par ailleurs prévue en cas d'opérations référendaires. À ce jour, cette procédure n'a quasiment jamais été mise en œuvre. Une application négative en a été faite par le juge des référés du tribunal judiciaire de Paris dans une ordonnance rendue le 17 mars 2019 (n°RG 19/53935) refusant d'ordonner, en période électorale, le retrait d'un message en ligne dénoncé comme inexact et trompeur.

Source : Réponse écrite au questionnaire de vos rapporteures, DACG, ministère de la Justice

● **Enfin, vos rapporteures considèrent que cet enjeu doit se traiter en « européens » et qu'il existe un véritable besoin de poursuivre et d'intensifier les coopérations avec nos partenaires en la matière.** Vos rapporteures se félicitent ainsi qu'en Moldavie, la France puisse mener des actions de *capacity building* en matière de lutte contre la désinformation en accompagnement sur la méthode à travers le développement du cadre juridique (l'État n'étant pas partie de l'UE, il n'est pas couvert pas le DSA ni le RGPD) et la mise à disposition d'une l'aide électorale (une personne déployée).

iii. L'enjeu de la préservation du modèle économique des médias traditionnels

Si les médias traditionnels ne sont pas exempts de biais, ils constituent un écosystème nécessaire pour permettre l'accès à une information de confiance.

● **Les représentants des médias auditionnés ont alerté vos rapporteures sur la mise en péril de leur modèle économique face à la concurrence des grandes plateformes et des contenus d'information relayés sur les réseaux sociaux.** Ils appellent de leurs vœux un meilleur partage de la valeur afin de garantir la rémunération d'un journalisme de qualité.

Selon RSF, les puissances parties à la guerre informationnelle mondiale usent largement des réseaux sociaux pour y déployer leurs opérations de manipulation. Les plateformes numériques structurent l'espace mondial de l'information et de la

communication, à la différence des médias qui l'occupent sans l'organiser. Leur infrastructure algorithmique pousse à la marge les contenus fiables (notamment de nature journalistique) au profit d'autres se distinguant essentiellement, non pas par leur fiabilité, mais par leur viralité. À l'occasion de la sortie de l'édition 2025 du Classement mondial de la liberté de la presse établi par RSF, il a été souligné que la fragilisation économique des médias constitue l'une des principales menaces pour la liberté de la presse.

Selon les informations fournies par France Médias Monde, le marché de la publicité – en particulier à l'international – est affecté par de profondes mutations, au premier rang desquelles l'essor des plateformes numériques, qui captent de plus en plus de parts de marché publicitaire (60 % du marché publicitaire français). Ces mutations impactent directement le niveau de recettes publicitaires de France Médias Monde, dépendant des algorithmes des plateformes. Cette évolution des revenus publicitaires, en partie captée par de nouveaux acteurs, constitue une forme de censure et tout au moins un risque d'éviction des médias « traditionnels ». Il s'agit d'un enjeu économique et démocratique majeur ; et d'une recommandation qui est d'ailleurs portée dans les conclusions des États généraux de l'information, qui proposent la mise en œuvre d'une contribution obligatoire des plateformes numériques sur la publicité digitale pour financer les médias d'information. Cet impératif de mieux partager la valeur doit aussi s'appliquer aux nouveaux acteurs de l'IA. En effet, les robots utilisant l'intelligence artificielle pour générer des contenus sont entraînés à partir de milliards de données issues d'éditeurs et de créateurs – et notamment des médias d'information – et il convient que l'Union européenne et la France se positionnent pour garantir un juste partage de la valeur entre les éditeurs qui produisent des contenus à valeur ajoutée (médias en particulier, etc.) et les entreprises qui les utilisent pour entraîner leurs modèles d'IA générative.

La préservation d'un écosystème médiatique fort est d'autant plus importante que nos compétiteurs consacrent des sommes très importantes à leur propre audiovisuel public à destination de l'étranger. Ainsi, le chercheur Maxime Audinet, auteur de *Un média d'influence d'État. Enquête sur la chaîne russe RT* (INA, 2021), auditionné par vos rapporteures, estime que la Russie consacre près de 500 millions d'euros par an à des médias d'État comme *RT* et *Sputnik*.

● **Le rôle de caisse de résonnance des manœuvres informationnelles que les médias peuvent jouer à leur insu constitue une raison supplémentaire pour les associer davantage à la stratégie de lutte contre les manipulations de l'information.** S'agissant des médias privés, les journalistes volontaires devraient pouvoir disposer de formations à la détection des manipulations de l'information, tout en proposant des briefings réguliers aux rédactions sur les campagnes de manipulations étrangères dont les services ont connaissance, pour éviter qu'ils s'en fassent le relais à leur insu.

Et ce, d'autant plus que les médias sont également victimes de la désinformation et de tentatives d'usurpation de l'identité pour propager de fausses

informations, parfois appelée « *typosquatting* ». En mars 2024, un détournement de RFI, utilisant tous les codes et les chartes de la radio mondiale, a été diffusé sur des boucles et réseaux sociaux russes pour faire croire à un risque d'épidémie de tuberculose en France, maladie « importée » par les soldats ukrainiens accueillis dans nos hôpitaux pour y être soignés. Cette infox a été « *débunkée* » immédiatement sur les antennes et réseaux sociaux de RFI (y compris en russe et en ukrainien) et de France 24.

Face au désengagement des plateformes en matière de soutien au *fact-checking*, RSF estime que l'Union européenne pourrait également prendre le relais en soutenant financièrement les médias professionnels dans leur mission de *fact-checking* et de « *débunkage* » sur le numérique, conformément au « bouclier démocratique européen » souhaité par la Commission européenne.

● **Alors qu'une partie du financement des campagnes de désinformation passe par de la publicité ciblée, la responsabilisation des annonceurs constitue un axe d'effort important.** Comme indiqué *supra*, une analyse de NewsGuard et Comscore montre que la mésinformation bénéficie de 2,6 milliards de dollars de revenus publicitaires estimés versés aux diffuseurs de mésinformation et de désinformation chaque année par les annonceurs programmatiques [(1)]. Ces données soulignent l'ampleur du financement involontaire de la mésinformation et de la désinformation en ligne par les grands annonceurs, qui placent leurs publicités sur des milliers de sites en utilisant la publicité programmatique, un processus complexe et informatisé qui laisse les marques dans le flou quant aux endroits où leurs publicités apparaissent et aux types de messages qu'elles financent. **En conséquence, RSF suggère que, sur le même modèle que la Responsabilité Sociétale des Entreprises (RSE), une Responsabilité Démocratique des Annonceurs soit introduite, ces derniers portant une responsabilité dans la situation économique du journalisme.** Il s'agirait d'inciter les annonceurs à conditionner leurs investissements publicitaires à des critères de fiabilité et d'éthique journalistique. L'alignement des stratégies publicitaires avec l'intérêt général est un levier décisif pour un écosystème médiatique sain et relève d'une nécessité démocratique.

Enfin, pour mobiliser davantage l'écosystème privé, une solution pourrait consister à intégrer la résilience informationnelle aux critères pris en compte au titre de la responsabilité sociétale des entreprises (RSE). En effet, il convient de responsabiliser les entreprises qui, trop souvent, contribuent à leur insu à financer la désinformation au travers des revenus publicitaires.

(1)Matt Skibinski, Newsguard, "Rapport : La publicité sur les sites de mésinformation ». (lien).

Recommandation : intégrer la résilience informationnelle aux critères pris en compte au titre de la responsabilité sociétale des entreprises (RSE), notamment s'agissant des annonceurs, afin de responsabiliser les entreprises qui, trop souvent, contribuent à leur insu à financer la désinformation au travers des revenus publicitaires.

● De nombreuses mesures visant à renforcer l'écosystème médiatique et à lutter contre la désinformation figuraient déjà dans les recommandations des États généraux de l'information. **C'est pourquoi, vos rapporteures seront vigilantes à leur pleine prise en compte dans le cadre d'un projet de loi « États généraux de l'information » dédié, comme cela pu être annoncé.**

iv. La piste de la certification de l'information de qualité

Afin de s'assurer de la valorisation d'un journalisme de qualité, vos rapporteures considèrent que la certification de l'information constitue une piste de réflexion à étudier. **L'objectivité de l'outil doit néanmoins être garantie pour s'assurer de sa crédibilité et se prémunir d'une instrumentalisation.**

Selon le Premier ministre, dans son discours d'ouverture du forum de VIGINUM le 28 mars 2025, l'État doit garantir l'accès de tous les citoyens à une information de qualité, afin que la conversation démocratique puisse se tenir. Dans *L'Étrange défaite*, Marc Bloch souligne d'ailleurs la nécessité pour l'État de garantir « *ce minimum de renseignements nets et sûrs sans lesquels aucune conduite rationnelle n'est possible* ».

La *Journalism Trust Initiative* (JTI) promue par RSF consiste ainsi à identifier, au bout d'un processus rigoureux de certification, les médias engagés dans une démarche de transparence et de responsabilité déontologique vis-à-vis de leurs audiences.

En retour, RSF plaide pour que ceux-ci soient récompensés de leurs efforts :

– par les citoyens: plus de confiance et de transparence amenant plus d'audience ;

– par les pouvoirs publics: à travers, par exemple, l'attribution des aides publiques ;

– par les annonceurs: à travers le fléchage des dépenses publicitaires vers des médias de confiance certifiés JTI ;

– par les plateformes numériques: à travers une promotion algorithmique des contenus diffusés par ces sources fiables d'information, ce qui permet aussi de contrer la désinformation sur les réseaux sociaux et de rendre effectif le droit à l'information. Faute de pouvoir miser sur une action volontaire de la part des plateformes, RSF porte la proposition d'introduire, dans la loi une obligation faite aux plateformes entrant dans le champ du *Digital Services Act* (DSA) d'amplifier

les médias identifiés comme fiables sur le fondement de la JTI ou de normes équivalentes.

d. La société civile en première ligne

En matière de protection de l'intégrité de l'espace informationnel, la société civile se doit d'être en première ligne, chaque citoyen devant devenir acteur de la défense informationnelle.

Vos rapporteures sont convaincues du fait que pour accélérer la résilience informationnelle de la Nation, il convient d'accueillir toutes les bonnes volontés issues de la société civile, y compris celles venues du secteur privé.

i. Poursuivre les efforts visant à bâtir un écosystème de confiance et à rendre les citoyens acteurs de la défense de l'espace informationnel

Pour augmenter la résilience de la Nation, il paraît indispensable que les institutions, la société civile et les entreprises travaillent de concert pour créer un écosystème de confiance. Dans la cybersécurité, une telle démarche a très bien fonctionné autour de l'ANSSI : les différents acteurs se connaissent et utilisent tous le même vocabulaire (les mêmes définitions et procédures). Il ressort des auditions menées que ce n'est pas encore le cas dans le domaine de la lutte contre les manipulations de l'information.

Selon vos rapporteures, il convient prioritairement de progresser sur la définition commune des concepts, de renforcer la coordination entre civils et militaires mais également d'inclure les entreprises, suivant une logique d'animation de réseau.

● Si VIGINUM joue un rôle important dans la résilience d'ensemble de la Nation, vos rapporteures estiment que ce dernier gagnerait encore à être renforcé et que les différentes initiatives existantes pourraient être rassemblées dans un souci de lisibilité.

Actuellement, dans les actions menées par VIGINUM, quatre axes peuvent être identifiés, selon les informations fournies par le service à vos rapporteures : informer ; outiller ; former et assister les partenaires étrangers.

– Informer : les rapports de VIGINUM permettent d'accroître le niveau de vigilance du grand public sur le niveau de menace ;

– Outiller : VIGINUM développe des outils en interne pour garantir la maîtrise souveraine de son analyse, qui ont le plus souvent vocation à être transmis au grand public, qu'il s'agisse de son métadétecteur ou de son outil de détection de la technique *copy-pasta* ;

– Formation : mise à disposition de ressources pédagogiques à destination des enseignants et des jeunes publics ;

– Former et assister les partenaires étrangers : actions de *capacity building* ; renforcement de l'expertise et développement de capacités crédibles et opérationnelles.

Par ailleurs, VIGINUM a entamé une démarche de rapprochement avec les acteurs de la société civile, notamment le monde académique et scientifique, afin de partager la connaissance sur la menace informationnelle et contribuer au renforcement de l'expertise française. Faisant le constat de l'absence d'un grand rassemblement de l'ensemble des acteurs investis dans la lutte contre les manipulations de l'information, VIGINUM et le SGDSN organisent chaque année un Forum afin de favoriser les rapprochements entre les administrations, les médias et les initiatives de la société civile.

Vos rapporteures considèrent que ces forums d'échange sont clés car il convient de créer des synergies entre les mondes régaliens, les militaires et la société civile. Comme l'a indiqué Jean Cattan, secrétaire général du conseil national du numérique, auditionné par vos rapporteures, il convient de « *sortir du prisme de la défense et de la sécurité nationale.* » Toutefois, ces initiatives demeurent trop ponctuelles.

● Aussi, vos rapporteures souhaitent-elles soutenir le projet d'une Académie de la lutte contre les manipulations de l'information, porté par VIGINUM, qui pourrait structurer l'ensemble des dispositifs, afin de renforcer l'accompagnement des partenaires.

Cette académie devrait notamment permettre de capitaliser sur l'expertise acquise par VIGINUM, sa méthodologie et de les partager au plus grand nombre. L'ensemble des acteurs concernés et intéressés devrait pouvoir bénéficier, s'il le souhaite, de formations ciblées et adaptées à leurs besoins dans l'objectif d'instaurer un réseau. Selon Jean Cattan, il convient ainsi de travailler selon une logique de « cercles concentriques ».

Selon les informations fournies par VIGINUM à vos rapporteures, cette structure aurait trois missions principales :

– Concevoir, produire et mettre à disposition des ressources pédagogiques adaptées pour chaque public au profit de l'Éducation nationale, des médias, du grand public, des acteurs économiques et associatifs ;

– Développer et proposer une offre de *capacity building* pour les partenaires étrangers souhaitant se doter de capacités en matière de lutte contre les manipulations de l'information ;

– Développer et proposer une offre de formations en matière d'OSINT afin de doter la société civile, les entreprises et les administrations de capacités élémentaires en matière d'investigation numérique appliquée à la lutte contre les manipulations de l'information.

Recommandation : Mener à bien le projet de création d'une Académie de lutte contre les manipulations de l'information autour de VIGINUM en 2025, afin de rassembler les initiatives existantes pour sensibiliser le grand public et renforcer la lisibilité d'ensemble de la politique publique.

Par ailleurs, vos rapporteures estiment que le rôle de VIGINUM dans le cadre du projet d'académie pourrait être étendu. Au regard de la place jouée par les parlementaires dans le débat public, un référent « élus » pourrait être spécialement désigné au sein de l'Académie afin d'alerter les parlementaires sur les campagnes de manipulations de l'information en cours et de répondre à leurs demandes d'information en cas de besoin.

Recommandation : en cohérence avec les actions de sensibilisation de la société civile, renforcer le lien entre VIGINUM et le Parlement en créant un référent « élus » au sein de l'Académie de lutte contre les manipulations de l'information, à même d'alerter les parlementaires sur les campagnes de manipulations de l'information en cours et de répondre à leurs demandes d'information en cas de besoin.

● Il convient également de développer davantage les synergies entre les secteurs public et privé. Ces synergies se justifient doublement : d'une part, parce que les entreprises constituent des cibles des stratégies de désinformation et, d'autre part, parce qu'elles peuvent être en mesure de proposer des solutions technologiques.

D'une part, selon VIGINUM, en tant que victimes potentielles mais aussi relais d'informations, les entreprises et acteurs privés sont des acteurs essentiels de la lutte contre les ingérences numériques étrangères. En effet, du fait de l'exposition de leurs activités à l'étranger et de leur rôle implicite de représentation de la France, les entreprises françaises sont des cibles évidentes pour des campagnes d'atteinte réputationnelle. Là encore, l'exemple de la campagne de dénigrement dont a été victime Dassault, à la suite de la perte d'un ou plusieurs avions Rafale en constitue un exemple.

Ainsi, selon l'historien David Colon, les manipulations algorithmiques et l'essor de l'IA générative affectent directement les entreprises, qui se retrouvent « en première ligne dans la guerre de l'information ». « *Non seulement la désinformation leur coûte 39 milliards de dollars de pertes boursières par an, selon une évaluation récente, mais elles sont de plus en plus fréquemment les cibles de « raids numériques » coordonnés et d'appels à mener des actions physiques à leur encontre. Il est par conséquent dans l'intérêt même des entreprises de contribuer à la préservation de l'intégrité de l'environnement informationnel, d'une part en ne contribuant pas involontairement à la désinformation par un recours non maîtrisé à la publicité programmatique, et d'autre part en contribuant activement à la résilience de la société au titre de leur responsabilité démocratique en contribuant*

à l'effort commun de lutte contre les manipulations de l'information et ingérences étrangères [(1)]. »

Vos rapporteures considèrent que face à la faible prise de conscience de cette menace, il y a un impératif à sensibiliser les entreprises afin qu'ils anticipent mieux les attaques, notamment les petites et moyennes entreprises. L'enjeu de la communication résiliente des entreprises pour éviter d'être sujet de la désinformation devrait également être davantage mis en avant.

Recommandation : sensibiliser les entreprises au risque informationnel, afin qu'ils anticipent mieux les attaques et ne se fassent pas les relais à leur insu des manœuvres informationnelles, notamment les petites et moyennes entreprises.

D'autre part, vos rapporteures identifient le besoin d'une filière économique dédiée à la lutte contre les manipulations de l'information. La relative absence d'entreprises française spécialisées dans la lutte contre les manipulations de l'information et l'influence pourrait constituer à terme une vulnérabilité stratégique. La création d'un marché privé qui rendrait rentable la protection de notre espace démocratique doit être encouragée afin de pallier la problématique du financement.

Selon les informations fournies à vos rapporteures, des outils et des connaissances issues du secteur privé et de la société civile pourraient être davantage mis à profit dans le cadre de la L2I. Les acteurs privés peuvent en particulier présenter un intérêt dans le domaine de la veille numérique et de l'analyse de l'environnement informationnel. L'analyse de ces données permet d'identifier des vulnérabilités informationnelles. Elle peut également participer à la mesure des effets d'opérations. Néanmoins, le recueil de données en ligne pose des défis éthiques et juridiques pour les entreprises qui collectent des informations en sources ouvertes (OSINT). S'il était décidé d'exploiter le plein potentiel de l'OSINT, il conviendrait au préalable de clarifier le cadre juridique applicable. Selon les informations fournies à vos rapporteures, l'absence de règles claires nuirait aujourd'hui à la filière française, au profit de concurrents étrangers.

Malgré des initiatives à saluer comme le cercle Pégase, think tank créé en 2022 par Sopra Steria, qui vise à éclairer la réflexion et à sensibiliser, les initiatives issues du secteur privé demeurent peu nombreuses. Le think tank vise à construire un réseau de confiance avec les ministères régaliens, les organismes de recherche, les universités, l'industrie, les media et l'éducation**. Vos rapporteures considèrent qu'il convient de tendre vers la mise en place d'un écosystème industriel français dédié à la lutte contre les manipulations de l'information, constitué y compris de PME.**

(1) « Les réseaux sociaux sont devenus des armes de manipulation massive », David Colon, Les Echos, 27 mars 2025. (lien).

Recommandation : soutenir la structuration d'une filière économique souveraine dédiée à la lutte contre les manipulations de l'information.

Certaines entreprises proposent d'ores et déjà des outils novateurs comme Newsguard, société américaine créée par des journalistes, qui propose notamment une extension de navigateur permettant d'évaluer la crédibilité des sources en ligne en leur attribuant un score de fiabilité et de limiter son exposition aux contenus de désinformation sur internet. L'entreprise conduit également des audits des sociétés d'IA afin d'évaluer leur résistance à la désinformation. La stratégie pour l'IA pourrait notamment intégrer une dimension veille, alerte et outils de lutte contre les manipulations de l'information, tout en sensibilisant davantage les entreprises fournisseuses de modèles d'IA générative à l'enjeu d'intoxication des IA. Au-delà du problème de propagation des fausses informations en elles-mêmes, les IA contribuent également à augmenter la visibilité des sites du réseau. Ne sachant pas faire la différence entre les sources fiables ou non, elles pourraient pousser les utilisateurs à les considérer équivalentes à des médias traditionnels et fiables à force de citer pêle-mêle tous types de sources. Selon Chine Labbé, rédactrice en chef de Newsguard, l'enjeu est d'apprendre aux sociétés d'IA à identifier les contenus de propagande d'origine étatique pour les *débunker* en temps réel ou du moins à traiter ces sources différemment des sources fiables. Il convient de tendre vers des outils fiables et transparents et explicables, à l'image de l'ambition fixée par des collectifs pour une IA de confiance comme confiance.AI.

ii. Promouvoir et financer la recherche transdisciplinaire dans le champ informationnel

● La lutte contre les manipulations de l'information ne peut progresser sans s'appuyer sur une recherche scientifique transdisciplinaire.

Pour ce faire, il convient de soutenir financièrement les initiatives mais surtout de garantir l'accès des chercheurs aux données, tout particulièrement aux données de fonctionnement des algorithmes des réseaux sociaux ou à celles permettant d'expliquer le fonctionnement des systèmes d'IA. Comme l'ont indiqué vos rapporteures, plusieurs domaines de recherche semblent particulièrement prioritaires : qu'il s'agisse de l'évaluation scientifique de l'efficacité des méthodes utilisées pour sensibiliser les publics scolaires à la lutte contre la désinformation ou bien encore de la mesure des effets des stratégies de désinformation sur la société française ; deux domaines encore trop peu investigué mais pourtant essentiels.

Les personnes auditionnées ont mis en avant l'avantage de la fertilisation croisée que constitue le processus d'enrichissement mutuel par l'échange d'idées, de concepts et d'expériences entre différentes disciplines ou approches. L'historien David Colon, auditionné par vos rapporteures, avait notamment mis en avant la nécessité de mobiliser davantage les sciences cognitives à travers la création d'un centre de recherche transdisciplinaire associant mathématiciens sociaux, psychologues sociaux et des économistes comportementaux et chercheurs spécialisés pour étudier les menaces informationnelles dans une perspective

« d'innovation sociale » [(1)]. Il préconise également la création d'un « observatoire de défense informationnelle », qui s'appuierait en partie sur les savoir-faire de VIGINUM, dont les missions et les financements devraient être renforcés. Un tel organisme pourrait également être chargé de lutter contre les cyber-attaques et de former les personnels politiques, économiques, etc., voire le grand public, à ces enjeux. Vos rapporteures estiment que cette proposition s'incarne en partie dans le projet d'académie de lutte contre les manipulations de l'information, qui devra s'attacher à promouvoir la pluridisciplinarité (alliant experts du numérique, mathématiciens, épidémiologistes, sociologues, etc.)

● **Enfin, le changement de cap de la nouvelle administration américaine peut constituer une opportunité pour la France**. À l'heure où les États-Unis ont délibérément choisi de fermer leur agence dédiée à la lutte contre les manipulations de l'information, la France gagnerait à construire une politique d'accueil pour les chercheurs américains spécialisés.

Recommandation : Promouvoir et financer la recherche transdisciplinaire dans le champ informationnel.

iii. Décentraliser la politique de lutte contre les manipulations de l'information

Vos rapporteures considèrent qu'il convient de mieux valoriser les compétences des citoyens et d'accompagner les initiatives existantes dans les territoires.

● **D'une part, il semble important d'entamer une réflexion sur la décentralisation de la politique de lutte contre les manipulations de l'information** car la possibilité que VIGINUM soit un jour dissout ne peut entièrement être exclue.

Auditionné par vos rapporteures, Jean Cattan a notamment formulé plusieurs pistes en ce sens. Il propose de faire appel aux plus de 4 000 conseillers numériques présents sur le territoire. Créés initialement pour accompagner les citoyens dans leurs démarches et vers l'autonomie numérique, ils sont au contact de la population au quotidien. VIGINUM pourrait profiter du maillage territorial existant et de leur formation en matière cyber pour proposer des modules de sensibilisation à la lutte contre les manipulations de l'information. De la même manière, d'autres dispositifs existants pourraient être étendus à la lutte contre les manipulations de l'information, comme celui des « café IA » porté par le Conseil national du numérique, démarche nationale qui vise à créer espace de débat sur l'IA. Ces formations pourraient également être ouvertes aux TPE/PME qui le souhaitent.

● **D'autre part, au regard de l'expérience britannique qui donne une place importante aux réservistes, il pourrait être envisagé de créer une réserve**

(1) « La défense psychologique face aux manipulations de l'information », David Colon, Revue Défense Nationale, n° 876, janvier 2025.

de spécialistes du champ informationnel afin de démultiplier les moyens de l'État. Au-delà de renforcer l'acceptabilité de la politique menée au sein de la population, les armées pourraient bénéficier de profils possédant des compétences d'analyse des données, de veille ou encore en communication civile ou en marketing digital.

Cette nouvelle réserve pourrait s'appuyer la réserve « cyber » prévue par la LPM 2024-2030 ou encore les dispositions de la loi la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN) instaurant une réserve citoyenne du numérique comme réserve thématique de la réserve civique. En effet, la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique consacre d'ores et déjà une réserve citoyenne du numérique « *ayant pour objet de concourir à la transmission des valeurs de la République, au respect de l'ordre public, à la lutte contre la haine dans l'espace numérique et à des missions d'éducation, d'inclusion et d'amélioration de l'information en ligne*. »

Recommandation : Décentraliser la politique de lutte contre les manipulations de l'information et créer une réserve de spécialistes du champ informationnel afin de démultiplier les moyens de l'État.

2. Prendre en compte la guerre cognitive, comme une composante majeure de la guerre de demain

La guerre cognitive, degré supérieur de la manipulation de l'information et concept encore méconnu dans le monde civil, pourrait pourtant constituer une des menaces à long terme pour les démocraties ainsi qu'une composante majeure de la guerre de demain.

a. La perspective du cerveau humain comme champ de bataille

Le terme « guerre cognitive » a été utilisé en 2017 par Vincent R.Stewart, directeur de la « *Defense Intelligence Agency* » américaine, lorsqu'il a déclaré que la guerre moderne était devenue une bataille cognitive [(1)].

● **Combinant sciences sociales et nouvelles technologies, le concept de guerre cognitive se distingue de la désinformation par son intention durable de modifier les mécanismes mêmes de pensée d'un individu ou d'un groupe social** (phénomènes d'ancrage, ciblage de populations jeunes via jeux vidéo par exemple sans attente de résultat immédiat, etc.).

(1) Underwood, K. (2017). Cognitive Warfare Will Be Deciding Factor in Battle. SIGNAL, 15 cité par. (lien).

Selon les informations fournies par le CICDE à vos rapporteures, la guerre cognitive fait du cerveau le nouveau champ de bataille en cherchant à agir sur le mode de pensée de l'adversaire, en façonnant ses émotions et modifiant ses croyances et ainsi ses actes et comportements. **Il ne s'agit plus ici de venir toucher et manipuler le message, mais bien les capacités cognitives elles-mêmes, et ainsi conditionner la pensée ou la non-pensée, jusqu'à paralyser l'action pour l'emporter.**

Ce concept, plus global, mêle différentes disciplines et vise donc à empêcher la capacité de décision et d'action. Ainsi, « *Derrière le processus réflexif c'est en fait le système de décision qui est la cible avec deux objectifs, soit le rendre prévisible, soit le paralyser* [(1)]. » **Il s'agit de paralyser le système sous l'effet de la double contrainte : c'est-à-dire « *lui imposer un choix impossible entre deux options également nuisibles* ».** « *Les démocraties occidentales risquent donc d'être paralysées par une double contrainte qui les conduit à l'inaction : soit ne pas intervenir afin de préserver la liberté d'expression au risque de s'exposer à des campagnes de déstabilisation de plus en plus massives, soit adopter une législation ou des mesures restrictives afin de contrôler les flux d'information au risque d'être accusé de censure* [(2)]. »

● **Chez nos compétiteurs et adversaires, la guerre cognitive constitue une stratégie hybride ayant pour objectif principal la manipulation des esprits, la subversion et donc la destruction des institutions démocratiques et de la démocratie en son cœur.** David Colon estime ainsi que « *La guerre cognitive est possible parce qu'un nombre considérable d'esprits sont devenus accessibles. Chaque génération a sa plateforme. TikTok est une fenêtre sur le cerveau des jeunes, en même temps que leur principale fenêtre sur le monde.* [(3)] ». Elle est déjà en partie une réalité : selon David Colon, « *Le renseignement russe a très tôt « capturé » cette technologie (…) L'Internet Research Agency d'Evgueni Prigojine, le fondateur du groupe paramilitaire Wagner, a eu recours au ciblage psychologique pour démultiplier le trolling, tout en enfermant des groupes d'internautes dans des chambres d'écho propices à l'exploitation de biais cognitifs, tels que l'effet de « vérité illusoire » découlant de la répétition de choses fausses, ou le biais de confirmation, voyant les individus privilégier les faits allant dans le sens de leurs idées préconçues* [(4)] ».

La Chine semble également avancée en la matière à travers la création de deux concepts : « *le premier est la « guerre intelligentisée », qui vise à accélérer la guerre cognitive en saturant l'espace informationnel de contenus. Le second est la « guerre cognitive algorithmique », qui désigne le recours à l'IA pour exercer une influence précise et individualisée à travers l'utilisation de données complètes sur*

---

(1) Collectif Thot, (2025). Entre « lutte informationnelle » et « guerre cognitive », la souveraineté en question Menaces sur la démocratie et sur le système de décision. Revue Défense Nationale, 876(1), 96-104. (lien).

(2) Ibid.

(3)Le Monde, David Colon, : « La guerre cognitive est possible parce qu'un nombre considérable d'esprits sont devenus accessibles », avril 2025. (lien).

(4) Ibid. (lien).

des populations cibles et l'instrumentalisation des algorithmes des plateformes. Tout cela vise à faire entrer les populations cibles dans ce que les Chinois appellent un « cocon informationnel » et, in fine, à remporter la guerre sans avoir à la mener. » (1) Héritière de la doctrine de la « guerre hors limites » elle vise à contrôler les croyances de l'ennemi par des messages ciblés ou un « engagement permanent » en exploitant les biais cognitifs et le ciblage. Ainsi, « *la propagande massive non ciblée et grossière si elle n'a pas disparue ne vise pas à produire les mêmes effets que l'approche cognitive qui est développée par la Chine. L'un cherche à diviser et s'imposer comme « ingénieur du chaos » en chef, l'autre cherche à modifier les croyances en profondeur* (2). » Pour se protéger, il est urgent de retrouver la maitrise des données.

SCHÉMA PRÉSENTANT LA RELATION CONCEPTUELLE ENTRE LA GUERRE COGNITIVE ET LES AUTRES TYPES DE GUERRE

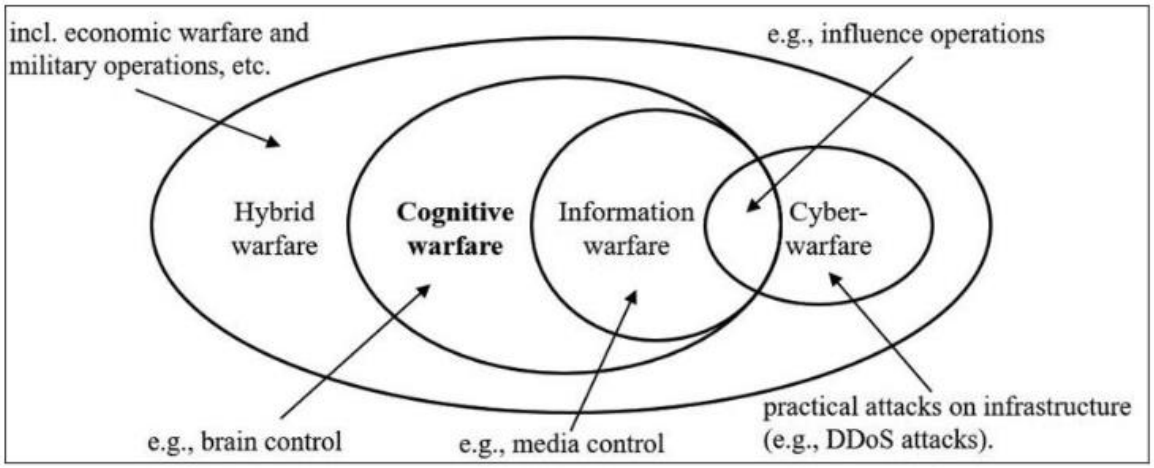


Figure 1. La relation conceptuelle entre la guerre cognitive et les autres types de guerre. Chaque type de guerre pourrait contenir l'élément d'influence et d'impact sur la cognition humaine, mais seule la guerre cognitive est spécifiquement dédiée au contrôle du cerveau et du cognitif en incorporant des neurosciences militarisées dans diverses pratiques.

Source : Note de recherche, Mme Bettina TRABELSI PEP/Observatoire des conflits, Commandement du combat futur, Armée de Terre, 10 octobre 2023.

b. Engager une réflexion sur les outils de « défense psychologique » ?

Si le concept de guerre cognitive est déjà pris en compte à travers notamment des travaux de prospective stratégique, vos rapporteures considèrent qu'il convient d'ores et déjà d'engager une réflexion sur les outils de défense possibles.

● Des travaux de prospective visent à établir les futurs possibles, à l'image du scenario de la *Red Team Défense* produit en 2021 « *Chronique d'une mort culturelle annoncée* », qui mettait en scène une opération militaire se tenant en 2050 dans laquelle la société était divisée en « zones de réalité alternatives

(1) Ibid.

(2 Bertrand Boyer, « Guerre cognitive algorithmique, gagner la guerre avant la guerre ? ». (lien).

communautaire » et où les armées françaises s'employaient à « sécuriser le réel » face à un adversaire capable de modifier les comportements des individus à grande échelle.

● Au plan militaire, comme l'indique le colonel David Pappalardo, il convient dès maintenant de se préparer à remporter la bataille de la cognition ce qui implique « *d'atteindre un niveau suffisant de sécurité cognitive* » dans la prise de décision individuelle, comme collective « *en se prémunissant contre nos propres certitudes, et en se protégeant contre les agressions qui visent nos perceptions*. » Cela implique notamment « *de faire émerger un C2 adapté à la dimension cognitive de la conflictualité multi-milieux multi-champs* [(1)] ».

Certaines initiatives existent d'ores et déjà doivent être encouragées comme la création de la matrice DIMA dans le cadre du projet M82 [(2)] conduit par Bertrand Boyer, qui vise à créer un cadre pour décrire les attaques cognitives et identifier les biais cognitifs les plus systématiquement exploités par un acteur afin de proposer des mesures de remédiation et de résilience. Le modèle repose sur quatre séquences (ou tactiques) qui correspondent chacune à une phase du traitement de l'information reçue par une cible. Ces quatre phases sont : détecter, informer, mémoriser, agir.

● **S'agissant de la société dans son ensemble, David Colon plaide en faveur de l'adoption d'une « stratégie nationale de défense psychologique » coordonnée par le SGDSN et inspirée des politiques menées par l'Agence suédoise de défense psychologique,** afin de mieux protéger la population contre les menaces informationnelles et d'améliorer la résilience de la société suédoise contre ces menaces hybrides en « *renforçant sa résistance psychologique* » [(3)]. Cette défense psychologique est un des quatre piliers de la doctrine de la « défense totale » mise en œuvre par la Suède (les trois autres piliers de cette défense étant la défense économique, civile et militaire). Toujours selon l'historien, la France demeure en retard dans ce domaine. Malgré la priorité accordée récemment par les pouvoirs publics à la lutte contre les ingérences et la mise en place d'une stratégie de résilience, l'aspect psychologique semble absent des stratégies françaises de défense contre les ingérences étrangères. Il considère notamment qu'il convient de mieux mobiliser les apports de la recherche scientifique en neurosciences.

---

(1) Les nouvelles formes de guerre, Le Rubicon, Colonel David Pappalardo, « la guerre cognitive : agir sur le cerveau de l'adversaire ».

(2)Lien vers la présentation de la plateforme « DIMA » issu du projet M82. (lien).

(3) « La défense psychologique face aux manipulations de l'information », David Colon, Revue Défense Nationale, n° 876, janvier 2025.

Recommandation : prendre en compte la guerre cognitive comme une composante clé de la guerre de demain et se préparer à mettre en place des outils de défense psychologique sur le modèle suédois.

3. Admettre que champs physiques et informationnels ne peuvent être entièrement décorrélés : « l'influence ne peut pas tout »

Enfin, malgré l'importance prise par le champ informationnel dans les conflits actuels et à venir, il convient d'admettre que les champs physiques et informationnels ne peuvent entièrement être décorrélés. Aussi, l'influence ne peut-elle pas tout. Les efforts préconisés par vos rapporteures en la matière sont indissociables des efforts de réarmement physique. **Vos rapporteures seront vigilantes à ce que les deux domaines ne soient pas opposés notamment dans le cadre des arbitrages budgétaires à venir, en particulier dans la perspective d'une actualisation de la loi de programmation militaire**.

● Comme l'indique le chef d'état-major des armées : « *Bien qu'immatérielle car ciblant les perceptions, l'influence n'est jamais déconnectée du réel et peut se faire par le truchement d'actions très concrètes. De fait, l'influence ne vit pas pour elle-même : elle est une caisse de résonance, un amplificateur positif comme négatif. Dans la lutte informationnelle, la synchronisation avec les autres actions stratégiques, opératives et tactiques est donc essentielle pour en tirer le meilleur parti.* » (1)

Ainsi, l'enjeu de la performance et de la masse des équipements ne peut être entièrement dissocié de la stratégie d'influence. En effet, l'influence dépend de la cohérence entre une posture, une action physique et un message. En conséquence, déclarer des choses qui ne correspondraient pas à une action réelle ou une capacité militaire crédible s'avèrerait contreproductif ; le risque de perte de crédibilité serait majeur.

● Pour autant, l'influence ne doit pas constituer la variable d'ajustement de la programmation budgétaire ; car comme le rappelait David Colon, auditionné par vos rapporteures, reprenant la logique russe, au regard de l'ampleur des effets produits, il est parfois aussi rationnel d'investir dans un influenceur que dans un char.

(1) Burkhard, T. (2023). Pas de stratégie sans influence, pas d'influence sans stratégie. Revue Défense Nationale, 856(1), 9-15. (lien).

EXAMEN EN COMMISSION

La commission procède à l'examen du rapport de la mission d'information sur « l'opérationnalisation de la nouvelle fonction stratégique influence » au cours de sa réunion du mercredi 2 juillet 2025.

La vidéo de la réunion est disponible sur le portail de l'Assemblée nationale en suivant le lien :

https://assnat.fr/6DCkg8

ANNEXE I : LISTE DES PROPOSITIONS

S’agissant de l’influence à destination de l’international

Recommandation n° 1 : Élaborer et publier une stratégie nationale d’influence clarifiant la définition des concepts, déterminant des priorités géographiques et visant à coordonner l’action des différentes administrations et partenaires au service de la politique d’influence.

Recommandation n° 2 : Clarifier les contours et le portage de la fonction stratégique influence dans l’actualisation de la RNS de 2025.

Recommandation n° 3 : Conforter le rôle de coordination du SGDSN dans une logique de rationalisation de l’organisation interministérielle, afin d’assurer la jonction entre les deux stratégies, d’une part d’influence, et d’autre part, de lutte contre les manipulations de l’information.

Recommandation n° 4 : Étudier l’opportunité d’élargir le COLMI à d’autres ministères y compris non régaliens (Culture, Éducation et Justice) et de créer un réseau de référents « influence » au sein des ministères pour s’assurer de la bonne prise en compte de la fonction stratégique.

Recommandation n° 5 : Organiser un débat associant les parlementaires, visant à déterminer les contours de l’aspect offensif de la stratégie d’influence et notamment le possible recours à des prestataires privés.

Recommandation n° 6 : accroître la coopération en matière hybride avec nos partenaires, en particulier approfondir notre partenariat avec les Britanniques.

Recommandation n° 7 : Poursuivre la mobilisation des missions de défense à l’appui de la stratégie d’influence des armées, en s’inspirant du modèle britannique.

Recommandation n° 8 : Renforcer la mobilisation du réseau des officiers insérés et de liaison ainsi que des élèves étrangers.

Recommandation n° 9 : En matière de communication à l'étranger, privilégier des campagnes de communication indirectes, pour créer de l'engagement et de l'impact sur les réseaux sociaux, en complément du recours aux relais institutionnels traditionnels.

Recommandation n° 10: S'assurer que les narratifs soient également diffusés en anglais et par différents moyens de communication pour garantir que la riposte soit largement diffusée et, au besoin, partagée rapidement avec les partenaires pour amplifier sa portée.

Recommandation n° 11 : Veiller à inclure la sensibilisation au risque informationnel et à l'influence au sein des formations des agents publics et à l'IHEDN.

Moyens humains et financiers

Recommandation n° 12 : Identifier plus clairement une filière « influence et lutte informationnelle » et la valoriser dans les parcours de carrière militaires et rendre obligatoire un passage dans les organisations internationales pour accéder aux plus hautes fonctions.

Recommandation n° 13 : Renforcer les moyens relatifs à la communication stratégique des services presse des ambassades et de la DCP, en faisait porter les efforts en direction du recrutement de profils spécialisés dans les stratégies d'influence afin de passer d'une communication institutionnelle à une véritable communication d'influence.

Recommandation n° 14 : Consolider les moyens de l'audiovisuel public à la hauteur des moyens consacrés par nos alliés et en tenant compte du désengagement américain.

Recommandation n° 15 : Renforcer les moyens humains à disposition de VIGINUM à hauteur de 20 ETP supplémentaires, en particulier s'agissant des fonctions de partenariats et d'ouverture vers la société civile.

Recommandation n° 16 : Identifier un « patch influence » dans la loi de programmation militaire et dans la stratégie nationale d'influence, précisant clairement les crédits et les effectifs alloués à l'opérationnalisation de la fonction stratégique influence et dont le suivi pourrait être assuré dans les documents budgétaires chaque année.

S’agissant de la lutte contre les manipulations de l’information

Recommandation n° 17 : Concevoir une doctrine de réponse claire en matière défensive et partagée au niveau de l’État, s’appuyant sur la définition de seuils de réponse, grâce à une meilleure connaissance de la mesure d’impact des stratégies de manipulations de l’information.

Recommandation n° 18 : Recourir à la déclassification de contenus de manière encadrée à l’appui de la démonstration du caractère erroné d’une manipulation de l’information et dans l’objectif de décrédibiliser l’action d’un compétiteur dans le cadre d’une manœuvre de riposte.

Recommandation n° 19 : Enrichir le rapport au Parlement prévu par la loi du 25 juillet 2024 sur les ingérences étrangères en y intégrant un état des lieux de la menace en matière informationnelle et en y incluant les ingérences numériques étrangères.

Recommandation n° 20 : Passer de la lutte contre les manipulations de l’information à la lutte contre les manipulateurs de l’information. Au-delà des actions de riposte menées dans le seul champ informationnel, renforcer les sanctions et mobiliser tous les leviers à disposition de l’État afin d’augmenter le coût des manœuvres informationnelles pour leurs auteurs, dans une logique de dissuasion.

Recommandation n° 21 : Poursuivre et amplifier la construction de partenariats pour permettre à l’ensemble des partenaires qui le souhaitent de bénéficier de l’expérience de VIGINUM, en faisant un effort particulier sur les partenaires les plus fragiles.

Recommandation n° 22 : Encourager et soutenir les travaux de recherche scientifique visant à objectiver les conséquences des ingérences informationnelles étrangères sur la société française, afin de ne pas surestimer ni sous-estimer la menace, voire risquer d’amplifier l’effet déstabilisateur sur nos sociétés des stratégies menées par nos compétiteurs.

Recommandation n° 23 : À court terme, encourager les actions de *débunking* et surtout de *prebunking,* prises comme des outils parmi d’autre dans la lutte contre les manipulations de l’information, tout en demeurant conscients de leurs limites.

Recommandation n° 24: À moyen et long termes, investir de manière croissante dans la construction de la résilience de la Nation à travers le renforcement de l’éducation aux médias et à l’esprit critique, en cohérence avec l’accroissement de l’investissement consenti en faveur des capacités de détection et de caractérisation de la menace informationnelle.

Recommandation n° 25 : Intégrer un volet sur l'EMI au guide de résilience devant être distribué à aux Français en 2025 et étudier l'opportunité de mettre à profit la journée nationale de la résilience et la journée de défense et de citoyenneté pour mener des actions de sensibilisation plus larges.

Recommandation n° 26 : Étudier la nécessité de compléter le droit existant pour lutter plus efficacement contre les ingérences numériques étrangères en période électorale ou a minima d'instaurer une coopération formalisée entre VIGINUM et la CNCCEP, dans la perspective des prochaines élections présidentielles.

Recommandation n° 27 : Mener à bien le projet de création d'une Académie de lutte contre les manipulations de l'information autour de VIGINUM en 2025, afin de rassembler les initiatives existantes pour sensibiliser le grand public et renforcer la lisibilité d'ensemble de la politique publique.

Recommandation n° 28: en cohérence avec les actions de sensibilisation de la société civile, renforcer le lien entre VIGINUM et le Parlement en créant un référent « élus » au sein de l'Académie de lutte contre les manipulations de l'information, à même d'alerter les parlementaires sur les campagnes de manipulations de l'information en cours et de répondre à leurs demandes d'information en cas de besoin.

Recommandation n° 29 : Sensibiliser les entreprises au risque informationnel, afin qu'ils anticipent mieux les attaques et ne se fassent pas les relais à leur insu des manœuvres informationnelles, notamment les petites et moyennes entreprises.

Recommandation n° 30 : Intégrer la résilience informationnelle aux critères pris en compte au titre de la responsabilité sociétale des entreprises (RSE), notamment s'agissant des annonceurs, afin de responsabiliser les entreprises qui, trop souvent, contribuent à leur insu à financer la désinformation au travers des revenus publicitaires.

Recommandation n° 31 : Soutenir la structuration d'une filière économique souveraine dédiée à la lutte contre les manipulations de l'information.

Recommandation n° 32 : Promouvoir et financer la recherche transdisciplinaire dans le champ informationnel, notamment en matière de mesure des effets.

Recommandation n° 33 : Décentraliser la politique de lutte contre les manipulations de l'information et créer une réserve de spécialistes du champ informationnel afin de démultiplier les moyens de l'État.

Recommandation n° 34 : Prendre en compte la guerre cognitive comme une composante clé de la guerre de demain et se préparer à mettre en place des outils de défense psychologique sur le modèle suédois.

ANNEXE II : AUDITIONS ET DÉPLACEMENTS DES RAPPORTEURES

(Par ordre chronologique)

1. Auditions

- **Ministère des armées – État-major des armées – M. le général de division Jean-Michel Meunier**, conseiller influence et lutte informationnelle du chef d'état-major des armées et chef du pôle « anticipation stratégique et orientation » ;

- **Secrétariat général de la défense et à la sécurité nationale (SGDSN) – M. Gwénaël Jézéquel**, conseiller pour les relations institutionnelles et la communication, **M. Yann Briand**, sous-directeur affaires internationales et **M. Gabor Arany**, sous-directeur adjoint de la planification de sécurité nationale ;

- **Ministère de l'Europe et des affaires étrangères – M. Christophe Lemoine**, porte-parole et directeur de la communication et de la presse, accompagné de **Mme Zalc-Muller** ;

- **M. David Colon**, historien, professeur agrégé d'histoire à l'Institut d'études politiques de Paris ;

- **Ministère des armées – État-major de la Marine nationale – M. le contre-amiral Cédric Chetaille**, adjoint du sous-chef d'état-major « opérations » ;

- **Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) – M. Benoît Loutrel**, membre du collège de l'ARCOM, président du groupe de travail « Supervision des plateformes en ligne » ;

- **Ministère des armées – État-major de l'armée de l'air et de l'espace – M. le général de division aérienne Pierre-Stéphane Vaysse**, sous-chef d'état-major « activité » ;

- **Ministère des armées – Commandement de la cyberdéfense (COMCYBER) – M. le contre-Amiral Vincent Sébastien**, adjoint au commandant de la cyberdéfense ;

- **Ministère des armées – Mme Olivia Penichou**, directrice de la délégation à l'information et à la communication de la Défense (DICOD) ;

➢ *Table ronde :*

– M. Laurent Cordonier, docteur en sciences sociales, directeur de la recherche de la Fondation Descartes, Paris – chercheur associé au GEMASS, Sorbonne Université – CNRS ;

– **Mme Christine Dugoin-Clément**, chercheuse à la Chaire Risques de l'IAE Paris-Sorbonne, à l'Observatoire de l'Intelligence Artificielle de Paris 1 Panthéon-Sorbonne, au centre de recherche des écoles de Saint Cyr Coëtquidan (CREC) et à celui de l'École des officiers de la Gendarmerie nationale (CREOGN) ;

➢ **Ministère des armées – Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE) – Mme Chloé Debiève**, chargée de domaine Influence et lutte informationnelle ;

➢ **Ministère des armées – État-major de l'armée de Terre – M. le général de division Damien Wallaert**, sous-chef d'état-major « opérations aéroterrestres » ;

➢ **Ministère des armées – Direction générale des relations internationales et de la stratégie (DGRIS) – M. Alexandre Escorcia**, chef du service Europe, Amérique du Nord et action multilatérale ;

➢ **M. Jean Cattan**, secrétaire général du Conseil national du numérique, et **M. Gwenael Jézéquel**, conseiller relations institutionnelles et communication du Secrétariat général de la défense et de la sécurité nationale (SGDSN) ;

➢ **Ministère de la Justice – Direction des affaires criminelles et des grâces – Mmes Laureline Peyrefitte**, directrice, et **Léa Obadia**, rédactrice au bureau de la lutte contre la criminalité organisée, le terrorisme et le blanchiment ;

➢ *Table ronde :*

– Mme Marie-Christine Saragosse, présidente de France Médias Monde, accompagnée de **MM. Thomas Legrand Hedel**, directeur de la communication, des relations institutionnelles et de la RSE, et **Corentin Masclet**, responsable des relations institutionnelles ;

– **M. Thibaut Bruttin**, directeur général de Reporters sans frontières, accompagné de **M. Antoine Bernard**, directeur du plaidoyer et de l'assistance.

➢ **Ministère de l'Europe et des affaires étrangères – Mme Marie-Doha Besancenot**, conseillère communication stratégique au cabinet de M. Jean-Noël Barrot, ministre de l'Europe et des affaires étrangères ;

➢ **X France – Mme Claire Dilé**, directrice des affaires publiques ;

➢ *Table ronde :*

– M. le général Bruno Courtois, conseiller Défense et Cyber, Sopra Steria, représentant le Cercle Pégase, accompagné de **M. David Olivier** ;

– Mme Chine Labbé, rédactrice en chef et vice-présidente senior chargée des partenariats, Europe et Canada, Newsguard.

➢ **Cabinet du Premier ministre – M. le colonel Nicolas Meunier**, conseiller Terre, Cabinet militaire, **Mme Caroline Ferrari**, conseillère diplomatique, cheffe de pôle et **Mme Julie Moulas**, conseillère presse ;

➢ **Direction générale de la sécurité intérieure – Mme Céline Berthon**, directrice générale ;

➢ *Table ronde :*

– M. Serge Barbet, directeur du CLEMI (Centre pour l'éducation aux médias et à l'information) ;

– **M. Jean Hubac**, chef de service de l'accompagnement des politiques éducatives et adjoint à la directrice générale de la DGESCO, ministère de l'Education nationale et de la jeunesse.

➢ *Table ronde – chercheurs à l'Institut de recherche stratégique de l'École militaire (IRSEM):*

– M. Paul Charon, directeur du domaine Influence et renseignement ;

– **Mme Maud Quessard**, directeur de directrice du domaine « Europe, Espace Transatlantique, Russie » ;

– **M. Maxime Audinet,** chercheur « Stratégies d'influence ».

2. Déplacements

➢ Déplacement à Bruxelles (le 4 février 2025)

– Représentation permanente de la France auprès de l'Union européenne – M. Sacha Baudinet, conseiller cyber-hybride et manipulations de l'information ;

– Institut de recherche stratégique de l'école militaire (IRSEM) - Antenne Europe – M. Philippe Perchoc, chef de l'antenne Europe ;

– Parlement européen – Mme Nathalie Loiseau (FR-Renew), présidente de la Commission spéciale sur le bouclier européen de la démocratie ;

– Service européen pour l'action extérieure (SEAE) – Mme Aude Maio-Coliche, directrice chargée de la communication stratégique et de la prospective ;

– OTAN – **Mme Marie-Doha Besancenot**, secrétaire générale adjointe pour la diplomatie publique.

➢ Déplacement à Londres (le 10 mars 2025)

– Échanges avec les membres de la mission de défense et de la chancellerie politique ;

– MI5 – échanges avec des représentants de la *Joint State Threat Assessment Team* ;

– **Ministère de la Défense britannique (MOD),** échanges avec **Mr. Luke Pollard,** *Parliamentary under-secretary of State*, des représentants du *Dep. Dir Global Defense Network* et du *Directorate for Defence Communications and Military Strategic Effects*;

– Parlement britannique - Mr. Gordon McKee, Mr. Calvin Bailey – députés de la Chambre des communes;

– Foreign, Commonwealth and Development Office (FCDO) – Mme Rachel Goodwill, directrice adjointe et responsable du département de la lutte contre les manipulations de l'information.

➢ Déplacement sur le site de VIGINUM à Paris (le 6 mai 2025)

– Échanges avec **M. Marc-Antoine Brillant**, chef de service de VIGINUM ;

– Rencontre avec les équipes.