N° 1454

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

SEIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale

le 29 juin 2023

N° 810

SÉNAT

SESSION ORDINAIRE DE 2022-2023

Enregistré à la Présidence du Sénat

le 29 juin 2023

RAPPORT PUBLIC

FAIT

AU NOM DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

*relatif à l'***activité** *de la* **délégation parlementaire** *au* **renseignement**
pour l'année **2022-2023**,

Par

M. Sacha HOULIÉ,

Député

Déposé sur le Bureau de l'Assemblée nationale

par M. Sacha HOULIÉ,

Déposé sur le Bureau du Sénat

par M. Christian CAMBON,

Président de la délégation

Premier vice-président de la délégation

SOMMAIRE

___

Pages

AVANT-PROPOS 9

CHAPITRE I^ER : BILAN D'ACTIVITÉ DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT DE JUILLET 2022 À JUIN 2023 13

I. UNE COMPOSITION SENSIBLEMENT RENOUVELÉE AU LENDEMAIN DES ÉLECTIONS LÉGISLATIVES DE JUIN 2022 13

II. UNE ACTIVITÉ SOUTENUE AU COURS DE L'ANNÉE ÉCOULÉE 15

III. LES DOCUMENTS TRANSMIS À LA DÉLÉGATION 18

IV. LE SUIVI DES PRÉCÉDENTES RECOMMANDATIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT 22

A. L'ÉTAT DE MISE EN ŒUVRE DES RECOMMANDATIONS DU DERNIER RAPPORT ANNUEL DE LA DPR 22

B. LE SUIVI DES RECOMMANDATIONS DES RAPPORTS ANTÉRIEURS À 2021 24

CHAPITRE II : LES ENJEUX D'ACTUALITÉ LIÉS À LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT 27

I. PRINCIPAUX ENSEIGNEMENTS DES RAPPORTS ANNUELS RELATIFS À LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT (EXERCICES 2021 ET 2022) 27

A. LES ENJEUX ET SUJETS D'INTÉRÊT DE LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT 27

B. L'ADAPTATION DE LA DOCTRINE DU RENSEIGNEMENT 28

1. La refonte du Plan national d'orientation du renseignement (PNOR) 28

2. La mise à jour du Plan d'action contre le terrorisme (PACT) 28

3. Le lancement des réflexions sur la lutte contre les ingérences étrangères 28

C. LES DONNÉES RELATIVES À L'ACTIVITÉ ET AUX RESSOURCES LIÉES AU RENSEIGNEMENT 29

1. Une diminution des productions écrites des services de renseignement en 2021 et 2022 29

2. Les ressources budgétaires et humaines 29

a. Les ressources budgétaires 29

b. Les ressources humaines 30

3. Les techniques de renseignement 31

II. LE VOLET RENSEIGNEMENT DE LA LOI DE PROGRAMMATION MILITAIRE POUR LES ANNEES 2024 À 2030 32

III. UNE NOUVELLE AMBITION POUR LE RENSEIGNEMENT FISCAL 34

CHAPITRE III : LE RENSEIGNEMENT, CŒUR BATTANT DE LA RIPOSTE DÉMOCRATIQUE AUX INGÉRENCES ÉTRANGÈRES 37

I. LES INGÉRENCES ÉTRANGÈRES EN FRANCE : UNE MENACE PROTÉIFORME, OMNIPRÉSENTE ET QUI S'INSCRIT DANS LA DURÉE 37

A. LES INGÉRENCES ÉTRANGÈRES, RÉVÉLATRICES D'UN CHANGEMENT D'ÉPOQUE 37

1. Un terreau favorable aux ingérences étrangères 37

2. Les formes multiples d'ingérences étrangères 39

a. Les formes classiques 39

b. Les formes modernes 39

c. Les formes hybrides 41

B. LA PLURALITÉ DES MODES OPÉRATOIRES MOBILISE TOUT LE SPECTRE DU RENSEIGNEMENT 42

1. La « signature » russe 43

2. La Chine et sa stratégie du « front uni » 45

3. La Turquie et ses velléités d'emprise 48

4. L'Iran et sa diplomatie des otages 49

5. Nos alliés n'agissent pas toujours comme des amis 50

C. DES VULNÉRABILITÉS PERSISTANTES 52

1. Notre naïveté 52

a. La sensibilisation des élus nationaux et locaux 52

b. La sensibilisation des entreprises 53

c. La sensibilisation du monde académique 54

2. L'insuffisant niveau de sécurité des systèmes d'information, publics comme privés 55

3. Les difficultés d'accès au financement des entreprises 56

4. Nos valeurs démocratiques : notre force et notre faiblesse 57

II. LA NOUVELLE PRIORITÉ DONNÉE À LA CONTRE-INGÉRENCE OUVRE UN NOUVEAU CYCLE DU RENSEIGNEMENT 60

A. UN CHANGEMENT DE PARADIGME POUR LA COMMUNAUTÉ DU RENSEIGNEMENT 60

1. La redéfinition des priorités stratégiques du renseignement au vu du contexte nouveau 60

2. De nouvelles façons de travailler 62
B. UNE GOUVERNANCE ADAPTÉE ET MODERNISÉE POUR RÉPONDRE AUX DÉFIS POSÉS PAR LES INGÉRENCES ÉTRANGÈRES 64
1. La répartition des rôles au sein de la communauté du renseignement 64
a. Les trois services compétents en matière de contre-espionnage et de contre-ingérence 64
i. Les signaux faibles mais fiables de Tracfin 67
ii. L'apport du renseignement douanier 69
b. Le rôle de la CNLRT 70
2. Les structures partenaires des services de renseignement 70
a. Le SGDSN et les agences qui lui sont rattachées : l'ANSSI et VIGINUM 70
i. L'ANSSI 70
ii. VIGINUM 71
b. Le SISSE 72
3. Une dimension interministérielle renforcée 73
C. DES MOYENS DE DETECTION ET D'ENTRAVE MULTIPLES MAIS ENCORE INSUFFISANTS 76
1. Une « boîte à outils » pour contrecarrer les ingérences étrangères 76
a. Le recours aux techniques de renseignement 76
b. Les mesures d'ordre diplomatique 78
c. Les mesures pénales 78
d. Les mesures d'ordre économique 79
e. Le dispositif de protection du potentiel scientifique et technique de la nation (PPST) 81
f. Les dispositions issues de la loi « séparatisme » du 24 août 2021 confortant le respect des principes de la République 83
2. Des nouveaux moyens d'entrave sont nécessaires pour contrecarrer des actions hostiles à nos intérêts fondamentaux 85
a. Permettre au ministre des Armées de s'opposer au recrutement par un État ou une entreprise étrangère de militaires nationaux détenteurs de savoir-faire militaires opérationnels rares 85
b. Instaurer un dispositif législatif spécifique aux ingérences étrangères, à l'instar de ce qui existe dans certains pays 87
c. Expérimenter l'extension aux finalités 1 et 2 de la technique de l'algorithme 89
d. Élargir aux ingérences étrangères le périmètre de la procédure des gels d'avoirs .. 90
e. Apporter une réponse européenne aux tentatives de déstabilisation liées aux ingérences étrangères 91

III. LES POSITIONS STRATÉGIQUES FRANÇAISES À L'ÉPREUVE DES INGÉRENCES ÉTRANGÈRES EN AFRIQUE AUSTRALE ET DANS L'OCÉAN INDIEN 95

A. RENSEIGNER POUR DÉTECTER ET SURVEILLER LES PHÉNOMÈNES D'INGÉRENCES 95

1. Les raisons d'être d'un climat d'ingérences 95

a. Des États faillis 95

b. L'existence de liens historiques avec des puissances étrangères 96

c. Un contexte géopolitique singulier 98

2. La mise au jour de véritables stratégies d'ingérence 99

a. Les signaux faibles prémisses de futures ingérences 99

b. Vers une convergence des ingérences 101

B. LA CONTESTATION DES INTÉRÊTS FRANÇAIS DANS LA RÉGION PREND DES FORMES MULTIPLES 101

1. La contestation de la présence française 102

2. La contestation de la souveraineté française 104

C. ORIENTER NOTRE OUTIL DE RENSEIGNEMENT DANS UNE STRATÉGIE DE RIPOSTE AUX INGÉRENCES ÉTRANGÈRES HOSTILES 105

1. Renseigner pour mieux exploiter les faiblesses de nos adversaires 105

2. Occuper le terrain 107

a. Le projet de base de l'action de l'État en mer porté par la France à Diego-Suarez 107

b. L'identification de nouveaux partenaires 108

3. Renforcer notre dispositif de renseignement 108

CHAPITRE IV : RAPPORT GÉNÉRAL DE LA CVFS 111

I. LA PRÉSENTATION GÉNÉRALE DES FONDS SPÉCIAUX EN 2021 113

A. UN AJUSTEMENT À LA BAISSE DES DOTATIONS EN FONDS SPÉCIAUX POUR LES TROIS PRINCIPAUX SERVICES (DGSE, DGSI ET GIC) 113

B. UN TROISIÈME EXERCICE CONSÉCUTIF DE RÉDUCTION DU MONTANT GLOBAL DES DÉPENSES 114

1. La réduction des dépenses de la DGSE justifie, à elle seule, la baisse de 4,95 % des fonds spéciaux dépensés (82,92 M€) 114

2. Une sincérité budgétaire remise en cause en 2022 et à remettre à niveau par les services du Premier ministre pour les exercices suivants 115

3. L'analyse des typologies de dépenses fait de 2021 une année atypique 115

C. UNE RÉGULATION INÉGALE DU NIVEAU DE TRÉSORERIE IMMOBILISÉE, GAGÉE ET DISPONIBLE 115

II. LES OBSERVATIONS COMMUNES À L'ENSEMBLE DES SERVICES 116

A. LA NÉCESSITÉ D'UNE APPLICATION STRICTE DE LA DOCTRINE D'EMPLOI FACE À L'AUGMENTATION TENDANCIELLE DES FONDS SPECIAUX 116

B. LE POIDS PARFOIS DISPROPORTIONNÉ DES FRAIS BANCAIRES SUPPORTÉS PAR LES SERVICES 117

C. LA LEVÉE D'ANGLES MORTS AU CONTRÔLE DE LA CVFS 118

III. LE SUIVI DES RECOMMANDATIONS DE 2020 118

RECOMMANDATIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT AU TITRE DE SON RAPPORT ANNUEL D'ACTIVITÉ 2022-2023 125

EXAMEN PAR LA DÉLÉGATION 129

SYNTHÈSE DU RAPPORT 131

AVANT-PROPOS

Mesdames, Messieurs,

Singulière époque que celle que nous traversons, caractérisée par des ruptures brutales, une violence endémique et une imprévisibilité de chaque instant. Nos démocraties sont dans le viseur de régimes autoritaires qui font du combat contre l'Occident leur fonds de commerce. La révolution numérique vient bouleverser les rapports de forces entre les puissances, entre les acteurs publics et privés, jusque dans les interstices de notre vie quotidienne. En quelques mois, deux crises majeures – le Covid puis la guerre en Ukraine – auront balayé nos certitudes, révélé nos fragilités et rebattu les cartes.

Cette nouvelle donne, une nouvelle ère froide qui brouille nos repères et nos habitudes, n'est pas sans conséquences sur l'activité de nos services de renseignement, confrontés à la multiplication des fronts avec des assaillants de plus en plus aguerris et dotés de techniques toujours plus sophistiquées. La loi de programmation militaire pour les années 2024 à 2030 confirme la priorité donnée au renseignement avec cinq milliards d'euros supplémentaires consacrés aux moyens humains de nos services et à la montée en puissance de leurs capacités techniques.

La Délégation parlementaire au renseignement a choisi de consacrer son rapport annuel au sujet des ingérences étrangères qui constituent des leviers de déstabilisation sans précédent de nos sociétés démocratiques. À la différence de la Commission d'enquête de l'Assemblée nationale « *relative aux ingérences politiques, économiques et financières de puissances étrangères visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques* », et dont le rapport a été publié le 1er juin 2023, la DPR s'est intéressée au rôle et aux moyens dont

disposent les services de renseignement français pour détecter, surveiller et entraver ces ingérences étrangères. Au-delà d'une analyse de la menace, il s'agit de présenter et d'évaluer l'écosystème du renseignement construit pour protéger notre pays des ingérences étrangères, dans le respect des principes et des règles d'un État de droit. En d'autres termes, en quoi le renseignement est-il le cœur battant de la riposte démocratique aux ingérences étrangères ?

Au-delà du thème central de son rapport annuel, la Délégation parlementaire au renseignement a également, au cours des douze derniers mois, exercé sa mission de contrôle et d'évaluation de la politique publique du renseignement à travers de nombreuses auditions et déplacements dans les services. Elle a aussi pris l'initiative, conjointement avec la commission nationale de contrôle des techniques de renseignement (CNCTR) d'organiser un colloque qui a rassemblé plusieurs centaines de participants le 11 mai 2023 dans la Galerie des Fêtes de l'Assemblée nationale, sous le haut-patronage des présidents des deux chambres, sur le thème : « *La politique publique du renseignement est-elle bien contrôlée ?* », et dont les actes font l'objet d'une publication spécifique de la Délégation parlementaire au renseignement.

Le présent rapport se décline autour de quatre chapitres :

- Le bilan d'activité de la Délégation de juillet 2022 à juin 2023 (I).

- Les enjeux d'actualité liés à la politique publique du renseignement (II).

- Le renseignement, cœur battant de la riposte démocratique aux ingérences étrangères (III).

- La présentation des travaux de la Commission de vérification des fonds spéciaux (CVFS) portant sur l'exercice budgétaire 2021 (IV).

***

Information au lecteur :

Nonobstant son souci de répondre à une légitime attente de transparence des citoyens, les membres de la Délégation parlementaire au renseignement sont soumis au respect du secret de la défense nationale.

C'est pour parvenir à concilier ces deux impératifs antagonistes qu'il a été décidé de produire un rapport public masquant les contenus classifiés « secret défense » au moyen d'un signe typographique (*****) invariable quelle que soit l'ampleur des informations rendues ainsi illisibles.

CHAPITRE I^ER : BILAN D'ACTIVITÉ DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT DE JUILLET 2022 À JUIN 2023

I. UNE COMPOSITION SENSIBLEMENT RENOUVELÉE AU LENDEMAIN DES ÉLECTIONS LÉGISLATIVES DE JUIN 2022

Lors de la réunion du 28 juillet 2022, il a été procédé à la reconstitution de la Délégation parlementaire au renseignement pour tenir compte du résultat des élections législatives des 12 et 19 juin 2022.

La composition de la Délégation s'en est trouvée profondément modifiée avec quatre nouveaux député(e)s, membres de droit ou désigné(e)s par la Présidente de l'Assemblée nationale appelé(e)s à siéger pour la première fois au sein de la Délégation parlementaire au renseignement. Aucun changement n'est intervenu s'agissant de la représentation des sénateurs.

Conformément à l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958, les députés membres de droit sont le Président de la Commission des lois et le Président de la Commission de la défense et des forces armées, à savoir MM. Sacha Houlié et Thomas Gassilloud, tous deux appartenant à la majorité présidentielle (Groupe Renaissance).

La loi prévoit que deux autres député(e)s sont désignés par la Présidente de l'Assemblée nationale pour la durée de la mandature « *de manière à assurer une représentation pluraliste* ». Au vu de la composition singulière de l'Assemblée nationale issue des élections législatives de juin 2022, la désignation des deux député(e)s non membres de droit a dû tenir compte de plusieurs facteurs :

– La prise en compte des équilibres politiques tant au sein de l'Assemblée nationale que de la Délégation parlementaire au renseignement dans son ensemble, du fait de sa composition bicamérale qui reflète aussi les forces politiques représentées au Sénat.

– L'objectif d'une composition la plus proche possible de la parité.

– L'ouverture de la DPR à des député(e)s issus d'autres commissions que celles représentées par les deux membres de droit.

Dans ces conditions, le choix de la Présidente de l'Assemblée nationale s'est porté sur :

– Mme Constance Le Grip, députée (Renaissance) des Hauts-de-Seine

– Mme Caroline Colombier, députée (Rassemblement national) de la Charente.

C'est la première fois depuis la création de la DPR qu'y siège un représentant du Rassemblement national. La question s'est posée de savoir quel groupe d'opposition devait être représenté au sein de la Délégation. C'est au vu de la composition au Sénat, où ne siège aucun membre de la majorité présidentielle, trois sénateurs LR et un sénateur SER que la Présidente de l'Assemblée nationale a fait le choix de nommer une députée issue du Rassemblée national.

S'agissant de la députée membre du groupe majoritaire « Renaissance », elle est issue de la Commission des finances qui n'était jusqu'à alors pas représentée au sein de la DPR qui a pourtant à connaître de l'usage des fonds spéciaux à travers la Commission de vérification des fonds spéciaux dont quatre de ses membres font partie.

La composition de la Délégation parlementaire au renseignement au cours de l'année écoulée fut donc la suivante :

<u>*Membres de droit*</u> :

- *Président* : M. Sacha Houlié, député (Renaissance) de la Vienne, Président de la Commission des lois de l'Assemblée nationale.

- *1er vice-président* : M. Christian Cambon, sénateur (LR) du Val-de-Marne, Président de la Commission des affaires étrangères et de la défense du Sénat.

- M. Thomas Gassilloud, député (Renaissance) du Rhône, Président de la Commission de la défense et des forces armées de l'Assemblée nationale.

- M. François-Noël Buffet, sénateur (LR) du Rhône, Président de la Commission des lois du Sénat.

<u>*Membres désignés par M. le Président du Sénat*</u> :

- Mme Agnès Canayer, sénatrice (LR) de la Seine-Maritime.

- M. Yannick Vaugrenard, sénateur (SER) de la Loire-Atlantique.

Membres désignés par Mme la Présidente de l'Assemblée nationale :

- 2e vice-présidente : Mme Constance Le Grip, députée (Renaissance) des Hauts-de-Seine.

- Mme Caroline Colombier, députée (RN) de la Charente.

Il ressort ainsi de cette composition qu'avec trois représentants sur huit, la majorité présidentielle est minoritaire au sein de la Délégation, ce qui était déjà le cas sous la précédente législature.

Avec trois femmes et cinq hommes, la parité n'est pas atteinte mais cela est cohérent avec l'absence de parité au sein des deux assemblées.

Les membres de la DPR sont issus de trois commissions permanentes différentes : lois, défense et affaires étrangères, finances.

Au cours de sa réunion constitutive du 28 juillet 2023, la Délégation a également procédé à la reconstitution de la Commission de vérification des fonds spéciaux, composée de quatre de ses membres (deux députés et deux sénateurs), et dont la présidence a été confiée au sénateur Yannick Vaugrenard.

La composition de la CVFS reflète le pluralisme politique et l'équilibre entre l'Assemblée nationale et le Sénat mais aussi entre les différentes commissions permanentes représentées au sein de la DPR :

- M. Yannick Vaugrenard, Président sénateur (SER) de la Loire-Atlantique.

- Mme Agnès Canayer, sénatrice (LR) de la Seine-Maritime.

- Mme Caroline Colombier, députée (RN) de la Charente.

- Mme Constance Le Grip, députée (Renaissance) des Hauts-de-Seine.

II. UNE ACTIVITÉ SOUTENUE AU COURS DE L'ANNÉE ÉCOULÉE

Entre le 1er juillet 2022 et le 30 juin 2023, la Délégation parlementaire au renseignement a tenu 12 réunions et procédé à l'audition des directeurs des services de renseignement et structures de l'État en lien avec le sujet retenu pour son rapport annuel, à savoir la lutte contre les ingérences étrangères.

Le Président de la Délégation a également rencontré à l'occasion de sa prise de fonction, chacun des services de renseignement du premier cercle ainsi que le directeur du GIC et le directeur de l'Académie du renseignement.

La Délégation a tenu ses réunions dans la salle sécurisée qui lui est dédiée à l'Assemblée nationale ; elle a également effectué des visites dans les services ; à la DGSI, à la DGSE et à la DRSD.

Par ailleurs, le Président a effectué, du 16 au 22 avril 2023, un déplacement en Afrique du Sud, à l'île de la Réunion et à Madagascar sur la thématique des ingérences étrangères qui fait l'objet d'un développement spécifique dans le présent rapport (chapitre III).

Parmi les faits marquant de l'année écoulée, on retiendra en particulier :

L'accueil, le 5 octobre 2022, d'une délégation de députés allemands du Bundestag, membres du PKGr, la commission parlementaire chargée du contrôle de la politique publique renseignement.

L'organisation conjointe avec la Commission nationale de contrôle des techniques de renseignement (CNCTR) d'un **colloque, le 11 mai 2023, sur le thème : « La politique publique du renseignement est-elle bien contrôlée ? »**. Ouvert par la Présidente de l'Assemblée nationale, qui présida la Délégation parlementaire au renseignement en 2018-2019, ce colloque a réuni parlementaires, magistrats, services de renseignement, autorités administratives indépendantes et universitaires. Près de 400 personnes ont assisté aux débats qui se sont tenus dans la Galerie des fêtes de l'Assemblée nationale.

La question du contrôle de la politique publique du renseignement se pose avec d'autant plus d'acuité que l'évolution des menaces, permanentes et protéiformes, a conduit à renforcer les moyens budgétaires, humains et techniques alloués aux services pour accomplir leur mission. La tenue de ce colloque – dont les actes constituent le Tome 2 du présent rapport – aura contribué à la réflexion collective sur les contours et les perspectives de la politique publique du renseignement. En s'interrogeant sur les enjeux et les modalités de son contrôle, il s'agit aussi de garantir au citoyen que la communauté du renseignement agit dans le cadre démocratique d'un État de droit pour le protéger dans un monde toujours plus dangereux.

Réunions plénières de la DPR de juillet 2022 à juin 2023

Jeudi 28 juillet 2022 :

Reconstitution de la Délégation parlementaire au renseignement et de la Commission de vérification des fonds spéciaux, au lendemain des élections législatives des 12 et 19 juin 2022

Mercredi 5 octobre 2022 :

Échange de vues avec une délégation de députés du Bundestag, membres du PKGr, la commission parlementaire chargée du contrôle de la politique publique du renseignement.

Jeudi 13 octobre 2022 :

Déplacement à Direction générale de la sécurité intérieure (DGSI).

Jeudi 10 novembre 2022 :

Audition de M. Frédéric Charillon, politologue.

Audition de M. Joeffrey Celestin-Urbain, chef du service de l'information stratégique et de la sécurité économique (SISSE).

Jeudi 8 décembre 2022 :

Audition de M. Serge Lasvignes, Président de la Commission nationale de contrôle des techniques de renseignement (CNCTR).

Audition de M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale (SGDSN) et de M. Gabriel Ferriol, chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum).

Jeudi 16 février 2023 :

Audition de M. le Préfet Pascal Mailhos, coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT).

Audition de M. Guillaume Valette-Valla, directeur de Tracfin.

Audition de M. Florian Colas, directeur national du renseignement et des enquêtes douanières (DNRED).

Jeudi 9 mars 2023 :

Déplacement à la Direction générale de la sécurité extérieure (DGSE).

Jeudi 13 avril 2023 :

Déplacement à la Direction du renseignement et de la sécurité de la défense (DRSD).

Jeudi 11 mai 2023 :

Colloque co-organisé avec la CNCTR à l'Assemblée nationale sur le thème : « *La politique publique du renseignement est-elle bien contrôlée ?* ».

Mardi 16 mai 2023 :

Audition de M. Sébastien Lecornu, ministre des Armées.

Mardi 13 juin 2023 :

Audition de M. Nicolas Lerner, directeur général de la sécurité intérieure (DGSI).

Audition conjointe de MM. Florian Colas, directeur national du renseignement et des enquêtes douanières (DNRED) et Guillaume Valette-Valla, directeur de Tracfin.

Jeudi 29 juin 2023 :

Examen du rapport annuel d'activité et renouvellement du Bureau de la Délégation parlementaire au renseignement.

III. LES DOCUMENTS TRANSMIS À LA DÉLÉGATION

Au cours de la période allant du 1er juillet 2022 au 30 juin 2023, la Délégation parlementaire au renseignement a été destinataire d'un certain nombre de documents classifiés.

Au titre de la nouvelle disposition de l'article 6 *nonies* de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, issue de la loi du 30 juillet 2021, la Délégation s'est ainsi vue communiquer, le 1er août 2022, **la liste des rapports** de l'inspection des services de renseignement ainsi que rapports des services d'inspection générale des ministères portant sur les services de renseignement qui relèvent de leur compétence.

La liste transmise recense *****

La Délégation a également été destinataire le 30 décembre 2022, du rapport annuel d'activité des services de renseignement et des services mentionnés à l'article L.811-4 du code de la sécurité intérieure, au titre de l'exercice 2021 soit près d'un an après la fin de l'exercice concerné. La Délégation avait déjà fait part de ce délai excessif ce qui a conduit la CNRLT, en lien avec le secrétariat de la DPR, à repenser les modalités d'élaboration de ce rapport afin de gagner en efficacité et en réactivité. Selon les termes d'une note adressée par la CNRLT au Président de la DPR le 24 janvier 2023, « *le changement de méthode appelle toutefois une modification du calendrier habituel* » avec une diffusion du rapport par la CNRLT le 30 juin 2023**. Il est important que cette échéance puisse être tenue afin que le rapport annuel de la DPR puisse rendre compte de l'activité des services au cours de l'année n-1**.

Parmi les autres documents transmis à la DPR au cours de l'année écoulée figurent également :

- Une note classifiée du directeur de cabinet de la Première ministre datée du 6 janvier 2023, relative aux modalités d'extension aux URL de la technique de renseignement dite de l'algorithme.

- Sept notes de renseignement portant sur les menaces pour l'ordre public représentées par les groupes liés aux mouvances ultra, dont deux communes avec le service central du renseignement territorial (SCRT) et la direction du renseignement de la préfecture de police de Paris (DRPP), qui ont donné leur aval à leur transmission à la DPR.

- Les réponses à divers questionnaires adressés à la DGSE, la DGSI, Tracfin, la CNRLT et le SGDSN sur le thème des ingérences étrangères.

Les modalités de mise en œuvre du droit à l'information de la DPR appellent les observations suivantes :

- S'agissant de l'obligation de transmission de la liste des rapports d'inspection relatifs aux services de renseignement, introduite par la loi du 30 juillet 2021, **la Délégation s'est étonnée qu'aucune liste ne lui ait été transmise depuis le 1er août 2022** alors même qu'aux termes de la loi, cette transmission doit être semestrielle. Cela a conduit le Président de la Délégation à écrire au Coordonnateur national du renseignement et de la lutte contre le terrorisme, le 13 juin 2023, pour en obtenir la communication. Une seconde liste de rapports de l'inspection des services de renseignements a alors été transmise le 29 juin 2023 par la CNRLT pour la période allant du 1er juillet 2022 au 29 juin 2023. Cette liste fait état de deux rapports *****. Par ailleurs, **il serait appréciable, comme ce fut le cas pour la transmission du 29 juin 2023, que cette liste soit moins laconique dans le descriptif des rapports**. Au-delà de la mention des seuls intitulés, la Délégation sollicite d'être également informée du service dont émanent les rapports et de leur date précise **(Recommandation °1)**.

  Sur la base de la liste transmise en août 2022, la Délégation a sollicité du Gouvernement la communication du rapport consacré à ***** (par un courrier du président de la DPR à la Première ministre en date du 13 juin 2023).

- Les délais de transmission de notes classifiées peuvent se révéler anormalement longs (deux mois), pour des raisons essentiellement administratives, alors même que le principe de leur transmission a fait l'objet d'un accord politique du ministre et du directeur général du service concerné.

- Le caviardage de certaines notes classifiées est parfois tel qu'il n'y a plus de véritable intérêt à leur transmission.

- L'article 6 *nonies* de l'ordonnance du 17 novembre 1958 prévoit, depuis la loi du 30 juillet 2021, que « *la délégation peut, dans la limite*

de son besoin d'en connaître, solliciter du Premier ministre (…) *tout autre document, information et élément d'appréciation nécessaire à l'accomplissement de sa mission* ». En lien avec le sujet retenu pour son rapport annuel, la Délégation a ainsi sollicité du Gouvernement, le 15 mai 2023, la transmission d'un rapport de l'Inspection Générale des Finances, consacré aux ingérences étrangères dans le domaine de l'enseignement supérieur et de la recherche. Or, à la date d'examen du présent rapport, soit 90 jours après la demande, celle-ci est restée lettre morte, sans réponse ni positive, ni négative**. Cette absence de réponse est préjudiciable au travail parlementaire et tout simplement à l'application de la loi. Aussi la Délégation demande au Gouvernement de s'engager, dans le délai maximal d'un mois, à répondre aux demandes formulées au titre de l'article 6 *nonies* de l'ordonnance du 17 novembre 1958 (Recommandation n° 2)**.

- Enfin, l'article L-143-4 du code des juridictions financières, dans sa rédaction issue de l'ordonnance n° 2016-1360 du 13 octobre 2016 prévoit que « *le Gouvernement transmet à la délégation parlementaire au renseignement les communications de la Cour des comptes aux ministres portant sur les services de renseignement ainsi que les réponses qui leur sont apportées* ». Or, **aucun document n'a jusqu'à présent été transmis à la Délégation depuis l'entrée en vigueur de cette disposition**. Il a pourtant été porté à la connaissance de la Délégation l'existence d'une communication de la Cour des comptes qui aurait dû lui être transmise automatiquement, sans avoir à en solliciter la communication ce qui a néanmoins été fait par un courrier du Président de la Délégation parlementaire au renseignement au coordonnateur national du renseignement et de la lutte contre le terrorisme, en date du 13 juin 2023. En réponse à ce courrier, le coordonnateur national du renseignement et de la lutte contre le terrorisme a fait état, à sa connaissance, que d'une seule communication de la Cour des comptes aux ministres portant sur les services de renseignement, relative à la fonction « renseignement » du ministère de l'Intérieur, datant de 2021. Or la DPR n'en a pas été destinataire, ce qui devrait pourtant être le cas sans qu'elle n'ait à en faire la demande.

  D'une façon plus générale, il serait souhaitable que soit portée à la connaissance de la DPR l'existence de tout « *document, information et élément d'appréciation nécessaire à l'accomplissement de sa mission* ». **Il est en effet difficile de solliciter la transmission de documents dont on ignore l'existence** comme par exemple, un rapport commandé il y a plusieurs années par la CNRLT, intitulé « *Forces et faiblesses du renseignement français* » mais dont la Délégation parlementaire au renseignement n'a jamais eu

connaissance. **Il pourrait également être utile à la DPR de se voir communiquer des RETEX** qui, par définition, ne concernent plus des opérations en cours.

À l'inverse, il semblerait que **les rapports classifiés de la DPR et de la CVFS souffrent peut-être d'une diffusion trop limitée**. En effet, si l'article 6 *nonies* de l'ordonnance du 17 novembre 1958 indique à son point VI que « *la délégation peut adresser des recommandations et des observations au Président et de la République et au ministre* » et qu'« *elle les présente au président de chaque assemblée* », rien n'est écrit sur le champ des destinataires de ses rapports classifiés. Or il serait pertinent **d'ouvrir, avec la CNRLT, une réflexion sur ce sujet afin que les services de renseignement et diverses autorités puissent prendre connaissance des travaux exhaustifs de la DPR, dans le respect naturellement du secret défense et du besoin d'en connaître (Recommandation n° 3)**.

IV. LE SUIVI DES PRÉCÉDENTES RECOMMANDATIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

A. L'ÉTAT DE MISE EN ŒUVRE DES RECOMMANDATIONS DU DERNIER RAPPORT ANNUEL DE LA DPR

Dans son rapport annuel 2021-2022 consacré à la lutte contre la criminalité organisée, la DPR avait formulé 10 recommandations dont l'état de mise en œuvre est le suivant, à la date du 29 juin 2023 :

Recommandation n°1 : Accentuer la lutte contre la fraude à la TVA.
Statut : *Complètement prise en compte*

Justification des services : ***** et la lutte contre la fraude à la TVA figure en priorité. La fraude aux finances publiques et la lutte contre la fraude à la TVA constituent une priorité. Par ailleurs, le ministre chargé des Comptes publics a annoncé en mai 2023 un plan de lutte contre les fraudes sociales et fiscales et un renforcement des moyens dédiés (notamment DNRED et Tracfin)

Recommandation n°2 : Augmenter les moyens humains de la DNRED en matière de lutte contre les stupéfiants dans les ports.
Statut : *Non prise en compte*

Justification des services : *****

Recommandation n°3 : Accompagner la croissance de Tracfin afin de permettre un développement de ses compétences et une diffusion de son expertise en matière de blanchiment.
Statut : *Complètement prise en compte*

Justification des services : Le schéma d'emplois de Tracfin arbitré pour 2023-2027 prévoit la création de 70 ETP supplémentaires sur l'ensemble de la période (20 ETP en 2023, 15 ETP en 2024 et en 2025, 10 ETP en 2026 et 2027).

Recommandation n°4 : *****
Statut : *Partiellement prise en compte*

Justification des services : *****

Recommandation n°5 : *****
Statut : *Non prise en compte*

Justification des services : *****

Recommandation n°6 : Renforcer la fluidité du recours aux offices, en tant que chefs de file dans leur domaine de compétence respectif, aux services de renseignement spécialisés du premier cercle.
Statut : *Complètement prise en compte*

Justification des services : *****

Recommandation n°7 : Améliorer le recrutement et le traitement des sources humaines, en assurant la transmission des connaissances des agents recruteurs.
Statut : *En cours de prise en compte*

Justification des services : *****

Recommandation n°8 : Élever le niveau de priorité de la lutte contre la criminalité organisée dans le renseignement fourni par les services du premier cercle, dans le respect de leurs compétences.
Statut : *Complètement prise en compte*

Justification des services : *****

Recommandation n°9 : Renforcer les moyens de lutte cyber face au développement des nouveaux modes d'action de la criminalité organisée.
Statut : *Partiellement prise en compte*

Justification des services : *****

Recommandation n°10 : Développer les mesures de prévention de la corruption des agents et des autorités publiques.
Statut : *Partiellement prise en compte*

Justification des services : *****

Rapport 2021-2022

Complètement prise en compte	4	8
Partiellement prise en compte	3	
En cours de prise en compte	1	
Non prise en compte	2	
Non cotée	0	
TOTAL	**10**	

B. LE SUIVI DES RECOMMANDATIONS DES RAPPORTS ANTÉRIEURS À 2021

Rapport 2020-2021

Complètement prise en compte	8	17
Partiellement prise en compte	2	
En cours de prise en compte	7	
Non prise en compte	2	
Non cotée	1	
TOTAL	**20**	

Rapport 2019-2020

Complètement prise en compte	23	37
Partiellement prise en compte	7	
En cours de prise en compte	7	
Non prise en compte	12	
Non cotée	10	
TOTAL	**59**	

Rapport 2018

Complètement prise en compte	23	36
Partiellement prise en compte	10	
En cours de prise en compte	3	
Non prise en compte	1	
Non cotée	10	
TOTAL	**47**	

CHAPITRE II :
LES ENJEUX D'ACTUALITÉ LIÉS À LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT

I. PRINCIPAUX ENSEIGNEMENTS DES RAPPORTS ANNUELS RELATIFS À LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT (EXERCICES 2021 ET 2022)

La Délégation parlementaire au renseignement a été destinataire fin juin 2023 d'une synthèse intermédiaire du rapport annuel d'activité des services spécialisés de renseignement et des services mentionnés à l'article L. 811-4 du code de la sécurité intérieure. Ce document intermédiaire permet à la DPR de disposer de quelques indicateurs clés utiles pour comparer l'activité des services d'une année sur l'autre.

Le rapport annuel relatif à la politique publique du renseignement pour l'exercice 2021, avait pour sa part été communiqué à la délégation parlementaire au renseignement le 30 décembre 2022 par M. Hugues Bricq, coordonnateur par intérim. Il rappelle les caractéristiques principales du cadre d'action des services de renseignement qui était resté marqué, comme en 2020, par le contexte particulier de la crise sanitaire. Cet exercice 2021 fut celui de l'élaboration d'une nouvelle version du Plan national d'orientation du renseignement (PNOR), validée par le Conseil national du renseignement le 13 juillet 2021*****.

A. LES ENJEUX ET SUJETS D'INTÉRÊT DE LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT

En 2021 et 2022, les faits marquant de l'activité de renseignement ayant mobilisé les services tant du premier que du second cercle furent les suivants :

*****

Pour l'année 2022, le rapport annuel d'activité devrait identifier plusieurs enjeux pour les services de renseignement :

- Les enjeux juridiques liés aux jurisprudences de la Cour européenne des droits de l'Homme et de la Cour de justice de l'Union européenne.

- Les enjeux en matière de mutualisation technique.

Parmi les sujets d'intérêt de l'année 2022 le rapport en souligne deux : le conflit russo-ukrainien d'une part, et l'interconnexion des systèmes d'information des services du 1er cercle d'autre part.

Le rapport d'activité de l'année 2021 rappelle pour sa part que le Conseil national du renseignement avait adopté une nouvelle version du PNOR et le CNRLT avait vu ses prérogatives codifiées dans le code de la défense, et doté d'un Centre national de contre-terrorisme (CNCT).

B. L'ADAPTATION DE LA DOCTRINE DU RENSEIGNEMENT

1. La refonte du Plan national d'orientation du renseignement (PNOR)

*****

2. La mise à jour du Plan d'action contre le terrorisme (PACT)

L'évolution de la menace terroriste a nécessité la mise à jour du PACT dont la première version datait de 2018. Son actualisation visait à intégrer les nouvelles recommandations des services, notamment émanant de la DGSI, mais aussi de Tracfin pour prévenir, par exemple, l'utilisation de crypto-actifs à des fins terroristes. Il en est ressorti 43 mesures dont 11 d'entre-elles, revêtant une sensibilité particulière, ne peuvent être rendues publiques *****. Parmi d'autres mesures figurent la structuration du contre-terrorisme au ministère des armées, la poursuite de la pratique systématique par la CNRLT du Retex (retours d'expérience) en cas d'attentat, ou encore l'amélioration du dispositif de suivi des individus radicalisés présentant des troubles du comportement.

3. Le lancement des réflexions sur la lutte contre les ingérences étrangères

Les années 2021 et 2022 ont également été marquées par l'intensification de la problématique des ingérences étrangères, laquelle a connu des développements qui l'ont confirmée comme un sujet majeur d'actualité dont la Délégation parlementaire au renseignement s'est saisie.

Une réflexion a été lancée pour assurer une meilleure transparence des actions d'influences étrangères sur la vie publique (registre des représentants d'intérêt), déclaration d'intérêt auprès d'une administration à l'image de la législation américaine « FARA » (*Foreign Agents Registration Act*). L'année 2021 s'est concrétisée par la mise en place d'un plan de sensibilisation contre les ingérences étrangères et l'engagement de travaux pour une meilleure protection des savoirs et des savoir-faire dans l'enseignement supérieur et la recherche scientifique.

C. LES DONNÉES RELATIVES À L'ACTIVITÉ ET AUX RESSOURCES LIÉES AU RENSEIGNEMENT

1. Une diminution des productions écrites des services de renseignement en 2021 et 2022

Une nouvelle typologie des productions écrites des services de renseignement est entrée en vigueur en 2021 *****.

Si l'activité des services de renseignement se mesure par la production écrite, laquelle fut en baisse en 2022 ***** par rapport à 2021 ***** et 2020 ***** en raison d'un changement de périmètre des documents pris en compte, celle-ci s'apprécie également à l'aune des actions de prévention et de réduction des vulnérabilités, lesquelles, à l'inverse des notes, ont considérablement augmenté en 2021 (3,2 millions d'enquêtes diligentées contre 1,6 million en 2020 et 1,8 million en 2019). Deux facteurs expliquent cette progression : l'activité de la DGSI en matière de criblage institutionnel (1,66 million d'enquêtes) et pour les demandes de visa (1 million d'enquêtes) ainsi que le phénomène de rattrapage en 2021 des enquêtes qui n'auraient pas été instruites en 2020 pour cause de Covid et le développement des activités de signalement et de sensibilisation.

*****

2. Les ressources budgétaires et humaines

a. Les ressources budgétaires

Depuis les attentats de 2015, les crédits en fonds normaux consacrés au renseignement ont crû sans discontinuer pour atteindre 3,03 milliards d'euros en 2022, contre 2,77 milliards exécutés en 2021 (en léger repli par rapport aux 2,84 milliards de 2020).

Tous les services spécialisés du 1er cercle ont connu en 2022 une augmentation de leurs crédits même si le niveau de ceux de la DGSI, bien qu'en hausse par rapport à 2021, n'atteignent pas ceux historiquement hauts de 2020.

RESSOURCES BUDGÉTAIRES PAR SERVICE (1ER CERCLE)

	2018	2019	2020	2021	2022
DGSE	790,9	858,2	882,6	919,3	935,9
DGSI	399,9	415,8	529,0	452,9	485,0
DRM	199,3	202,1	202,6	208,9	210,8
DRSD	120,4	130,5	142,1	157,9	163,6
DNRED	73,4	72,6	75,5	76,7	83,0
TRACFIN	16,6	16,8	18,2	18,1	19,5
Total services du 1er cercle	**1 600,5**	**1 696,1**	**1 850,0**	**1 833,9**	**1 897,8**

En millions d'euros

En revanche, les services du second cercle mentionnés à l'article L. 811-4 CSI ont vu leurs crédits sensiblement diminués au cours de la période récente pour se situer à leur niveau le plus bas par rapport à 2018.

RESSOURCES BUDGÉTAIRES PAR SERVICE (2ND CERCLE)

	2018	2019	2020	2021	2022
SCRT	283,6	302,3	303,9	306,8	230,2
SDAO	17,7	18,4	19,5	19,4	20,4
DRPP	77,5	76,4	82,3	85,9	70,4
SNRP	17,7	21,6	14,0	13,3	14,8
Total services du 2nd cercle	**396,4**	**418,7**	**419,7**	**425,4**	**335,8**

En millions d'euros

S'agissant des fonds spéciaux, *****

b. Les ressources humaines

En matière de ressources humaines, le total des personnels tous services confondus (1er et second cercle avec les structures d'appui) s'est établi à 19 572 postes en 2022, en léger repli par rapport à 2021 (20 677 effectifs). En revanche, les effectifs des six services du 1er cercle augmentent *****. Ce sont donc logiquement les services du 2nd cercle qui voient leurs effectifs baisser sensiblement, en repli *****.

Les effectifs par catégorie révèlent la forte présences d'agents A et A+ dans les services du 1er cercle, et une majorité d'agents de catégorie B dans les services du 2d cercle.

Les services de renseignement du 1er comme du 2nd cercle emploient très majoritairement des hommes *****.

Le constat le plus notable est celui d'un recours de plus en plus accru à des personnels contractuels, conjugué à une baisse de la courbe des recrutements militaires.

Enfin, les données disponibles pour l'année 2021 font apparaître une augmentation de près de 12 % du nombre de jours de formation (86 125 jours en 2021 contre 77 025 en 2020), ce qui en année post-Covid traduit un réel investissement des services, ainsi que de l'Académie du renseignement (858 participants à des formations en 2021 contre 653 en 2020) qui poursuit un travail de diversification de ses publics formés notamment en direction des agents du second cercle, leur nombre ayant progressé de 14 en 2017 à 151 en 2021.

3. Les techniques de renseignement

La répartition des techniques de renseignement selon les finalités définies par le code de la sécurité intérieure montre que si la finalité 4 reste prédominante (32,8%), les finalités 2 (18,4%) et 3 (15,1%) connaissaient une hausse substantielle.

RÉPARTITION DES TECHNIQUES DE RENSEIGNEMENT PAR FINALITÉS DU CSI

(TOUS SERVICES)

Finalités	2021	2022
Finalité 1 Indépendance nationale, l'intégrité du territoire et la défense nationale	1 761	1 151
Finalité 2 Intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère	7 184	8 304
Finalité 3 Intérêts économiques, industriels et scientifiques majeurs de la France	4 122	6 831
Finalité 4 Prévention du terrorisme	16 043	14 767
Finalité 5a Prévention des atteintes à la forme républicaine des institutions	9	10
Finalité 5b Prévention des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 CSI	75	79
Finalité 5c Prévention des violences collectives de nature à porter gravement atteinte à la paix publique	6 044	5 767
Finalité 6 Prévention de la criminalité et de la délinquance organisées	6 526	6 739
Finalité 7 Prévention de la prolifération des armes de destruction massive	812	1 317
Prévention des évasions et sécurité des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues	134	108
TOTAL	**42 710**	**45 073**

II. LE VOLET RENSEIGNEMENT DE LA LOI DE PROGRAMMATION MILITAIRE POUR LES ANNEES 2024 À 2030

Le projet de loi relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, déposé à l'Assemblée nationale le 4 avril 2023, renforce sensiblement les moyens accordés à la communauté du renseignement avec une enveloppe budgétaire supplémentaire de 5 milliards d'euros sur la période. Si ces moyens nouveaux sont essentiellement orientés vers la DGSE, la DRM et la DRSD vont aussi bénéficier d'un doublement de leur budget.

La LPM introduit également un certain nombre de dispositifs juridiques visant à :

– **Permettre l'accès des services de renseignement au casier judiciaire au titre des enquêtes administratives de sécurité** *(article 40)*. Cet article autorise les services de renseignement à consulter le bulletin n° 2 du casier judiciaire, ce qui ne leur était jusqu'alors interdit dans le cadre des enquêtes administratives de sécurité menées en application de l'article L. 114-1 du code de sécurité intérieure. Or, dans le cadre des enquêtes d'habilitation, les services pouvaient être conduits à prendre des décisions administratives défavorables aux personnes concernées sur la base d'une simple mise en cause judiciaire inscrite au fichier des antécédents judiciaires mais qui aurait finalement donné lieu à un classement sans suite. Et a contrario, ils étaient également susceptibles de délivrer une habilitation à un individu sans connaître d'une éventuelle condamnation prononcée à son encontre.

– **Permettre la communication par l'autorité judiciaire aux services de renseignement des éléments d'une procédure ouverte pour crime de guerre ou crime contre l'humanité** *(article 43)*. En application des articles 706-25-2 et 706-105-1 du code de procédure pénale, les transmissions d'informations entre l'autorité judiciaire et les services de renseignement existent déjà pour ce qui relève des champs de la prévention du terrorisme, de la sécurité et de la défense des systèmes d'information et de la prévention de la criminalité et de la délinquance organisées. La loi de programmation militaire crée une nouvelle dérogation au principe du secret de l'enquête et de l'instruction de la procédure en élargissant aux enquêtes ouvertes pour crimes contre l'humanité ou crimes et délits de guerre la possibilité de partage de pièces de procédure entre autorité judiciaire et services de renseignement du premier cercle. Cette transmission d'information pourrait être de nature à permettre d'empêcher la fuite de criminels de guerre ou leur entrée sur le territoire de l'Union européenne.

– **Protéger l'anonymat des anciens agents des services de renseignement ou des anciens membres des forces spéciales dans le cadre des procédures judiciaires** *(article 44)*. En application de l'article 656-1 du code de procédure pénale, l'identité réelle des agents appartenant à certains services de renseignement du premier et du second cercle, dont le témoignage est requis au cours d'une procédure judiciaire sur des faits dont ils auraient eu connaissance lors de missions intéressant la défense et la sécurité nationale ne doit jamais apparaître au cours de la procédure judiciaire. Or le code de procédure pénale ne précise pas les conditions d'application dans le temps de ce dispositif de protection de l'identité réelle des agents concernés. Cette disposition de la loi de programmation militaire étend ainsi le bénéficie de cette protection aux anciens agents des services de renseignement et des forces spéciales ce qui les protège eux mais aussi potentiellement leurs collègues toujours en activité et par là-même l'action du service auquel ils appartiennent.

– **Garantir la prise en compte des intérêts fondamentaux de la Nation en cas d'activité privée en rapport avec une puissance étrangère** *(article 42)*. Si les articles présentés précédemment ont été adoptés sans modification par l'Assemblée nationale, cet article 42, dont l'objet a trait à des transferts de savoir-faire sensibles à des puissances étrangères, a donné lieu à plusieurs amendements adoptés en commission, puis en séance publique.

Il convient au préalable de rappeler qu'en l'état du droit actuel, il ne peut être fait obstacle au départ de militaires vers des pays ou des entreprises étrangères qui les emploieraient dans l'objectif même d'obtenir de leur part des informations ou savoir-faire à caractère stratégique *****. Ce phénomène ne semble pas propre à la France puisque les autorités britanniques ont indiqué qu'une trentaine de leurs pilotes avaient été approchés.

Ce sujet est d'autant plus difficile à cerner que si le droit pénal permet de punir ceux qui transmettent des informations confidentielles à des compétiteurs étrangers (articles 411-6 à 411-8 du code pénal), encore faut-il que cette livraison d'informations soit identifiée et poursuivie sur le plan pénal.

C'est pourquoi la loi instaure un régime de déclaration préalable auprès du ministre de la défense de tout projet d'exercice d'une activité à l'étranger dans le domaine de la défense ou de la sécurité permettra la vérification que cette activité ne comporte pas de risque de divulgation par l'intéressé de procédés opérationnels, de capacités techniques et de savoir-faire nécessaires à la préparation et à la conduite des opérations militaires, susceptible de porter atteinte aux intérêts fondamentaux de la Nation. Ce régime de déclaration emporterait plusieurs conséquences pour les intéressés en cas de refus du ministre : retrait de décoration, retenue de pension ne pouvant dépasser 50 % ainsi qu'un délit en cas de non déclaration ou de méconnaissance de l'opposition du ministre puni de 5 ans d'emprisonnement et de 75 000 euros d'amende.

Le Parlement a adopté plusieurs amendements tendant à inclure dans le périmètre le bénéfice direct ou indirect à un État ou une entreprise étrangère, les collectivités territoriales étrangères. Outre les militaires, seraient également concernés les agents civils de l'État ou de ses établissements publics participant au développement de savoir-faire nécessaires à la préparation et à la conduite des opérations militaires. En revanche, n'entreraient pas dans le dispositif les militaires qui souhaiteraient exercer une activité au sein d'une entreprise titulaire d'une autorisation d'exportation de matériel de guerre français.

III. UNE NOUVELLE AMBITION POUR LE RENSEIGNEMENT FISCAL

Le ministre des comptes publics, Gabriel Attal, a annoncé le 9 mai 2023, une série de mesures de lutte contre la fraude fiscale et douanière, parmi lesquelles figure la création envisagée d'une cellule de renseignement fiscal.

La lutte contre les fraudes fiscales et sociales figure de manière explicite dans la stratégie nationale du renseignement de juillet 2019.

Le renseignement fiscal relève à ce jour, au sein du ministère de l'Action et des comptes publics, de :

- Deux services de renseignement du 1er cercle : Tracfin et la Direction nationale du renseignement et des enquêtes douanières (DNRED).

- Un service d'enquêtes fiscales spécialisé, la direction nationale d'enquêtes fiscales (DNEF), échelon national d'action et de coordination du dispositif de recherche du renseignement fiscal.

Fin 2019, une *task force* opérationnelle dédiée au renseignement fiscal, associant ces trois structures, a été mise en place. Cette *task force* exploite des renseignements d'ordre fiscal qu'elle met en commun, autour de thématiques opérationnelles et partage toute information qui peut se révéler utile à l'identification de schémas complexes de fraude fiscale.

Néanmoins, les résultats obtenus par cette *task force* restent limités du fait d'angles morts liés aux spécificités de Tracfin et de la DNRED. En effet, si Tracfin bénéficie d'un champ large de compétence en la matière, ses moyens opérationnels sont limités tandis que c'est l'inverse pour la DNRED qui dispose de moyens opérationnels importants mais limités au champ restreint de la fiscalité douanière.

En annonçant la création d'une cellule dédiée au renseignement fiscal, le Gouvernement souhaite franchir une nouvelle étape et se donner des moyens adaptés pour lutter contre les grands schémas d'évasion et d'opacification fiscales.

Il s'agit de pouvoir détecter, par le renseignement, tout ce qui échappe jusqu'à présent aux filtres et systèmes d'alerte de notre régime déclaratif.

La Délégation parlementaire au renseignement salue le choix du Gouvernement de ne pas créer un service de renseignement supplémentaire, à part entière, dédié au renseignement fiscal. Il est en effet plus cohérent d'inscrire la montée en puissance de cette mission dans le périmètre actuel de la communauté du renseignement.

Pour autant, la Délégation s'interroge sur la décision de confier le portage de cette cellule à la DNRED plutôt qu'à Tracfin dont c'est tout de même le cœur de métier. La création d'une cellule de renseignement fiscal au sein de Tracfin aurait permis d'affirmer l'identité de ce service du premier cercle qui doit encore progresser en matière de culture du renseignement, comme en attestent régulièrement les travaux de la commission de vérification des fonds spéciaux.

Le calendrier de mise en place de cette cellule au sein de la DNRED prévoit la création d'une structure administrative en 2024 pour un début d'activité opérationnelle en 2025, une fois clarifiées les nombreuses questions juridiques qui se posent autour de cette nouvelle mission de renseignement.

Au titre de sa mission de « *suivi des enjeux d'actualité et des défis à venir qui s'y rapportent* », la Délégation demande au Gouvernement d'être associée aux travaux de préfiguration liés à la création de cette cellule de renseignement fiscal (**Recommandation n° 4**).

CHAPITRE III :
LE RENSEIGNEMENT, CŒUR BATTANT DE LA RIPOSTE DÉMOCRATIQUE AUX INGÉRENCES ÉTRANGÈRES

Le sujet de la lutte contre les ingérences étrangères a été le fil conducteur des travaux de la Délégation parlementaire au renseignement au cours de l'année écoulée. On a longtemps pensé que des conflits millénaires seraient solubles dans l'économie de marché. Or la réponse est négative et le réveil brutal pour nos démocraties occidentales, particulièrement vulnérables dans la confrontation globale qui s'opère sous nos yeux.

Les ingérences étrangères, parce qu'elles représentent une menace protéiforme, omniprésente et durable ouvrent un nouveau cycle du renseignement, cœur battant de notre riposte démocratique.

I. LES INGÉRENCES ÉTRANGÈRES EN FRANCE : UNE MENACE PROTÉIFORME, OMNIPRÉSENTE ET QUI S'INSCRIT DANS LA DURÉE

La France est une grande puissance politique, militaire, économique, scientifique, culturelle. Il n'y a rien d'étonnant à ce qu'elle fasse l'objet d'agressions protéiformes émanant de l'étranger, visant à infléchir ses positions, à saper sa cohésion nationale, à connaître ses intentions ou encore à voler ses savoir-faire. Ces puissances étrangères profitent également d'une forme de naïveté et de déni qui a longtemps prévalu en Europe, même si le retour de la guerre sur notre continent a permis une prise de conscience collective sur la nécessité de protéger notre souveraineté, dans toutes ses dimensions.

A. LES INGÉRENCES ÉTRANGÈRES, RÉVÉLATRICES D'UN CHANGEMENT D'ÉPOQUE

1. Un terreau favorable aux ingérences étrangères

Démêler le vrai du faux entre l'influence et l'ingérence n'est pas toujours chose facile tant la frontière peut se révéler ténue. 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 politique, juridique, militaire, économique et technologique.

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.

Le sujet des ingérences étrangères a toujours existé mais il prend une ampleur nouvelle ces dernières années pour au moins trois raisons :

D'abord, **un changement radical de contexte géopolitique**. Nous sommes brutalement passés d'un monde de compétition à un monde de confrontation entre d'un côté des régimes autoritaires et de l'autre des démocraties occidentales dont le leadership est contesté et que l'on veut faire passer en perte de vitesse. Ce clivage entre l'occident et le reste du monde s'impose comme le marqueur dominant de la période actuelle.

Ensuite, **la révolution numérique et technologique**. En quelques années, le cyberespace est devenu un champ privilégié de confrontation et de compétition stratégique entre les États. La Russie et la Chine, notamment, associent leur politique d'influence à une capacité d'espionnage et d'ingérence ainsi qu'à une maîtrise de l'outil numérique. Les menaces hybrides créent de l'ambiguïté dans un contexte géopolitique où les limites entre guerre et paix sont de plus en plus floues, donnant lieu à une zone grise où s'entremêlent les notions de compétition, contestation et d'affrontement.

Enfin, **un enchevêtrement des phénomènes** entre ce qui relève des affaires intérieures et extérieures, de structures publiques et privées mais aussi de logiques locales et globales. On observe une diversité croissante d'acteurs – étatiques ou non –, de modes opératoires et d'effets produits qui provoquent une grande confusion sémantique et compliquent la compréhension des phénomènes et la réponse à y apporter.

Le niveau de menaces d'ingérences étrangères se situe ainsi à un stade élevé, dans un contexte international tendu et décomplexé. Il résulte de la conjonction de tous ces facteurs, une intensification manifeste des ingérences étrangères, traduisant une forme d'hybridité que le Président de la République Emmanuel Macron évoquait en ces termes le 20 janvier 2023 lors de ses vœux aux armées : « *Ce qui caractérise les nouveaux conflits de notre siècle est sans doute le brouillage entre une conflictualité ouverte, explicite, et une malveillance répétée, systémique, pernicieuse. La guerre ne se déclare plus, elle se mène à bas bruit, insidieusement, elle est hybride.* »

2. Les formes multiples d'ingérences étrangères

Les ingérences étrangères s'opèrent de façon de plus en plus décomplexée et concernent tous les secteurs d'activité, de la vie démocratique à la vie économique, du monde de la recherche aux espaces numériques. Elles prennent des formes multiples : opérations de désinformation, cyberattaques, espionnage, opportunités juridiques liées à l'extraterritorialité, corruption, trahison, etc.

On peut répertorier les différentes formes d'ingérences dans trois catégories : classiques, modernes et hybrides.

a. Les formes classiques

Traditionnellement, les ingérences prennent la forme d'actions clandestines menées sur le territoire national par des puissances étrangères, par l'intermédiaire de leurs services de renseignement extérieur. Elles relèvent de l'espionnage et visent principalement à la captation d'informations stratégiques ou sensibles.

Au titre de ces formes classiques, on peut mentionner **les manœuvres d'approche des élites politiques et administratives**. Le *Qatargate* qui a frappé en plein cœur le Parlement européen à la fin de l'année 2022, a mis au grand jour un scandale de corruption de plusieurs députés européens, inédit par son ampleur et impliquant notamment le Maroc et le Qatar. Les élus, de toutes tendances politiques, sont clairement des cibles privilégiées.

L'affaire Pegasus avait elle aussi révélé le possible espionnage de nombreux dirigeants politiques jusqu'au sommet de l'État avec un téléphone portable du Président de la République potentiellement visé par le logiciel espion ainsi que ceux de 14 ministres en exercice.

L'**espionnage économique** relève également d'une forme traditionnelle d'ingérence. Chaque année, un nombre important d'entreprises et de laboratoires de recherche sont victimes d'actes d'espionnage pouvant entraîner une perte de compétitivité importante et altérer leur image. La Chine est la puissance étrangère de loin la plus active en matière d'espionnage dans les laboratoires de recherche scientifique notamment par des financements proposés à des structures universitaires de taille moyenne qui peuvent souffrir d'un manque de moyens et de reconnaissance.

b. Les formes modernes

Au gré des évolutions technologiques, les ingérences épousent des formes de plus en plus diverses et dématérialisées. **L'espace cyber est devenu un vecteur majeur d'ingérences étrangères** et le nombre de

cyberattaques causées par des acteurs hostiles, étatiques ou non, est en progression sensible ces dernières années. Les mondes physique et virtuel sont si étroitement liés qu'il est difficile de tracer une séparation nette entre les deux. La protection des informations ne concerne plus seulement les documents classifiés. On assiste à une forme d'arsenalisation des données à caractère personnel ou de la propriété intellectuelle, qui deviennent autant une cible qu'une arme dès lors qu'un acteur se les approprie.

Les services de renseignement étrangers s'appuient naturellement sur les opportunités offertes par le cyberespace pour collecter des données, manipuler l'information, saboter des infrastructures critiques. Il peut s'agir d'opérations entièrement cyber, qui mettent en œuvre un « **mode opératoire d'attaque cyber** » (MOA) qui, parce qu'il s'apparente à une boite à outils, est difficilement attribuable à ses opérateurs et à leurs commanditaires sans une investigation approfondie en renseignement. Un nombre croissant d'États possède aujourd'hui la capacité de commanditer des actions de cyberespionnage grâce à un ticket d'entrée devenu abordable, bénéficiant d'investissements conséquents et du développement d'un marché privé, avec des sociétés proposant des services de lutte informatique active. De plus, l'offre d'outils offensifs sur étagère, qu'ils soient proposés par des entreprises privées ou des groupes cybercriminels, se poursuit et contribue à la multiplication d'acteurs malveillants. On observe ainsi une tendance globale à la standardisation des techniques, tactiques et procédures des attaquants, parallèlement à l'industrialisation des écosystèmes cyber-offensifs à partir desquels les opérations sont menées. De plus, la cybercriminalité présente un risque systémique de par son ampleur et son impact sur le tissu économique national et sur l'activité des institutions publiques affectées, si l'on se réfère au ciblage d'hôpitaux et d'administrations qui pourrait davantage relever d'une volonté de déstabilisation que d'une logique financière crapuleuse.

Parmi les nouvelles formes d'espionnage figure également le **domaine spatial**. On se souvient du satellite russe *Luch-Olymp* espionnant en 2017 le satellite franco-italien de communications militaires sécurisées *Athena-Fidus*. Plus récemment, le 1er août 2022, quelques mois après l'invasion de l'Ukraine, Moscou a placé à 450 km d'altitude un nouveau satellite espion, Kosmos-2558, sur la même orbite qu'un satellite de l'armée américaine. Ce satellite « inspecteur » n'observe pas le sol mais son environnement ; il peut gêner sa cible, perturber sa mission ou encore l'espionner. Les conséquences de ces ingérences modernes peuvent se révéler très impactantes : captation de données, déni de service, satellites rendus « aveugles », désorbités voire détruits.

c. Les formes hybrides

Les objectifs des États les plus offensifs en matière d'ingérences ont évolué au cours de la période récente. Ils ne se limitent plus seulement à des atteintes aux intérêts fondamentaux de la Nation, mais s'apparentent de plus en plus à des opérations d'influence et de manipulation de l'information dans le but d'infléchir les prises de position politique d'un pays. Les moyens mis en œuvre par ces acteurs se sont considérablement développés grâce aux possibilités offertes par l'usage des technologies numériques.

Les **campagnes de manipulation de l'information à grande échelle** constituent ainsi la nouvelle forme, hybride, d'ingérence étrangère. Elles prennent une ampleur sans précédent, au point de représenter un défi pour les démocraties dans la guerre informationnelle et de réputation que leur livrent certains régimes autoritaires. Les fausses nouvelles sont les armes d'une guerre conduite contre l'occident sans que, pendant trop longtemps, nous en ayons réalisé l'ampleur et, surtout, que nous ayons identifié les moyens de nous défendre.

Quatre critères permettant de caractériser ces ingérences étrangères d'un genre nouveau :

– L'implication d'acteur(s) étranger(s).

– Un contenu manifestement inexact ou trompeur.

– Une amplification inauthentique fondée sur une diffusion des contenus de manière artificielle ou automatisée, massive et délibérée.

– Une atteinte aux intérêts fondamentaux de la Nation par la déstabilisation du fonctionnement démocratique.

Depuis le milieu des années 2010, un nombre croissant de pays démocratiques a fait l'objet de campagnes d'ingérence numérique étrangère sur les réseaux et médias sociaux lors d'échéances électorales majeures telles que l'élection présidentielle américaine de 2016 ou le référendum britannique sur le Brexit.

En France, la menace que font peser les manipulations de l'information, particulièrement dans le processus de décision démocratique, est apparue au grand jour à l'occasion de l'affaire dite des « *Macron Leaks* » de 2017, destinée à déstabiliser une candidature à l'élection présidentielle à quelques jours du second tour du scrutin. Celle-ci comprenait à la fois un volet cyber avec une attaque informatique débouchant sur un vol de données privées et un volet informationnel incluant la diffusion de rumeurs et de

fausses nouvelles. Il ne s'agit pas tant de défendre une ligne idéologique que de semer le doute et la confusion et altérer la confiance des citoyens dans leur système démocratique.

Les modes opératoires sont hybrides en ce qu'ils associent plusieurs leviers : médias à la main de puissances étrangères, pseudo ONG et think tank, outils techniques de diffusion de fausses informations sur les réseaux sociaux (faux comptes, robots, trolls) qui participent à une brutalisation du débat public.

Ces manipulations de l'information à grande échelle participent de la stratégie du *sharp power* qui, à la différence du *soft power*, ne vise pas à promouvoir un modèle et des valeurs mais consiste au contraire à nuire au modèle adverse, en l'affaiblissant et en le décrédibilisant de l'intérieur.

B. LA PLURALITÉ DES MODES OPÉRATOIRES MOBILISE TOUT LE SPECTRE DU RENSEIGNEMENT

La menace inspirée de puissances étrangères évolue d'une triple façon :

– Les missions dévolues aux services adverses ont évolué. L'espionnage *stricto sensu*, entendu au sens de la captation d'informations confidentielles, continue de perdurer mais tend à évoluer au profit d'actions d'interférence et de corruption du processus décisionnel.

– Ces missions sont confiées à un panel plus large d'acteurs. En effet, outre les services de renseignement, d'autres entités administratives étrangères sont sollicitées, ainsi que le secteur privé. Les réseaux d'associations, qui structurent les diasporas présentes sur le territoire national et garantissent le maintien du lien organique avec leur pays d'origine, constituent de fait de puissants vecteurs d'ingérence. Les administrations régaliennes d'une puissance étrangère, qui pilotent et instrumentalisent des représentations en France (lieux de culte, collectifs associatifs…) constituent également des vecteurs de séparatisme. Par ailleurs, les acteurs médiatiques qui ont investi le champ informationnel francophone relaient un narratif contribuant à dégrader l'image de la France.

– Les actions d'ingérence sont conduites à l'encontre de cibles plus diversifiées. Ainsi, à mesure que l'architecture de la décision politique a évolué en France après plusieurs vagues de déconcentration et surtout de décentralisation, l'attention de nos adversaires, jusque-là très focalisée sur Paris, s'est elle-même orientée vers l'ensemble du territoire.

***** Pour autant, d'autres « signatures » témoignent d'une pluralité de puissances étrangères à la manœuvre dans les actions qui ciblent notre pays.

1. La « signature » russe

Plusieurs modes opératoires sont caractéristiques d'une « signature » émanant de la Russie.

La première, historique, est l'infiltration. Si de nombreux services de renseignement étrangers sont présents en France de façon déclarée, il en est aussi qui agissent de façon clandestine sur notre territoire. C'est historiquement le cas de la Russie avec le FSB (Service fédéral de sécurité), le SVR (Service de renseignement extérieur) et le GRU (Service de renseignement militaire). La méthode à laquelle recourent les autorités russes consiste à infiltrer des officiers de renseignement sous couverture diplomatique, bénéficiant à ce titre d'une immunité.

Malgré les mesures d'entrave – expulsions et interdictions d'entrée sur le territoire – prises au lendemain de l'invasion de l'Ukraine marquées par l'expulsion de 41 officiers de renseignement russes sous couverture diplomatique, fort est de constater que le dispositif des services de renseignement russe en France demeure actif. *****

La DGSE a en revanche constaté une baisse de l'activité d'espionnage à l'étranger à la suite des vagues d'expulsion de membres des services russes en Europe et plus largement en Occident, après l'empoisonnement en 2018 de l'ancien membre du service militaire russe Sergueï Skripal et de sa fille Salisbury, puis bien sûr de l'invasion de l'Ukraine. La Russie a ainsi été privée d'une force de frappe en Occident de l'ordre de plus de 600 agents expérimentés sous couverture diplomatique. Ceci explique que les services russes s'efforcent de compenser cette perte par le déploiement d'illégaux ou de clandestins en Occident, qu'il est par nature difficile de quantifier, et se montrent également plus offensifs qu'auparavant sur les autres zones Afrique du Nord / Moyen-Orient ou en Asie.

La stratégie du pouvoir russe vise aussi à **attirer dans sa sphère d'influence d'anciens dirigeants européens à travers leur participation aux conseils d'administration de grands groupes russes** : L'ancien Premier ministre François Fillon a ainsi rejoint en 2021 les conseils d'administration de Zarubezhneft et de Sibur. L'ancien Chancelier allemand Gerhard Schröder, l'ancien Premier ministre finlandais Esko Aho ou encore l'ancien Chancelier autrichien Christian Kern et des anciens ministres autrichiens font partie des ex-dirigeants partis rejoindre de grands groupes russes. Tous, à l'exception de

Gerhard Schröder, ont démissionné après la déclaration de guerre russe à l'Ukraine.

Les opérations de **manipulation de l'information de grande ampleur** sont également, et depuis l'époque soviétique, une marque de fabrique des services russes et la tentative soviétique de désinformation la plus célèbre reste la théorie selon laquelle le Président Kennedy aurait été assassiné par la CIA. Sur ce segment informationnel, la Russie est ouvertement engagée dans une stratégie révisionniste et de contestation de l'ordre international, explicitement dirigée contre les pays occidentaux, et recourant à tous les champs de l'hybridité. La fermeture des médias russes en Europe (*Russia Today* et *Sputnik*) a permis de diminuer la portée de la guerre informationnelle conduite par la Russie mais celle-ci tend toutefois à redéployer des moyens en Afrique – pas seulement francophone – pour y relayer un discours anti-français.

Ces dernières années, avec l'essor des réseaux sociaux, **les manœuvres d'ingérence dans les processus électoraux** ont également pris une tout autre ampleur, comme le détaille ce rapport de 448 pages du procureur Robert Mueller sur l'ingérence russe dans la campagne présidentielle américaine de 2016. L'ingérence russe sur l'élection présidentielle américaine de 2016 s'est appuyée sur trois outils : des tentatives d'intrusion dans l'infrastructure des systèmes de vote, la diffusion d'e-mails du Parti démocrate volés par piratage ainsi qu'une campagne massive sur les réseaux sociaux.

Aux termes du rapport Mueller, il ne fait aucun doute que « *l'État russe s'est immiscé dans l'élection présidentielle de 2016 d'une façon systématique* (…) *D'abord, une organisation russe a mené une campagne sur les réseaux sociaux qui a favorisé Donald Trump et dénigré son opposante démocrate Hillary Clinton. Puis des hackers russes, émanant du service de renseignement militaire russe GRU, ont piraté des messages du parti démocrate et d'un proche d'Hillary Clinton, diffusés sur internet par des sites anonymes et par WikiLeaks, qui avait reçu les messages volés directement des Russes* ». Robert Mueller rapporte que des officiers du GRU ont « *ciblé pour la première fois le bureau personnel de Clinton environ cinq heures après la déclaration de Donald Trump du 27 juillet 2016* », lors de laquelle il avait appelé la Russie à retrouver les emails effacés de sa rivale en tant ce propos : « *Russie, si vous écou*tez »...

L'élection présidentielle américaine de 2016 n'est pas un cas isolé. Il ressort que la plupart des ingérences récentes dans des processus électoraux sont liées, de près ou de loin, à la Russie, à l'instar des « *Macron Leaks* » lors de l'élection présidentielle française de 2017. La Russie n'est certes pas le

seul acteur étatique à utiliser cette méthode de l'ingérence par la manipulation de l'information, mais c'est le seul qui l'a érigé en doctrine officielle et dont la stratégie assumée est d'affaiblir l'occident. L'élite politique et militaire russe n'hésite pas à utiliser le terme de « guerre de l'information » mais Moscou estime que ses actions sont défensives dès lors que la promotion des valeurs démocratiques et libérales et le soutien à la société civile sont considérés comme des actions subversives visant un changement de régime.

Le recours à des **entreprises militaires privées (SMP)** est également un mode opératoire caractéristique de la Russie. En 2012, Vladimir Poutine déclarait devant la Douma qu'« *une corporation d'entreprises militaires privées serait un outil efficace pour réaliser les objectifs nationaux sans faire appel à la participation directe de l'État russe* ». La plus connue de ces milices est le groupe *Wagner*, société de mercenaires russe créée par Dmitri Outkin, un ancien officier du GRU (renseignement militaire russe). Le groupe paramilitaire, dirigé par l'oligarque russe Evguéni Prigojine, est connu depuis 2014 pour son implication dans le conflit en Ukraine puis son intervention en Syrie un an plus tard, dans le sillage de l'armée russe. Officiellement, *Wagner* n'existe pas en Russie où les sociétés privées militaires sont interdites. Mais en réalité, ce groupe illégal est un instrument géopolitique au service de Moscou, très présent notamment en Afrique. L'envoi de « volontaires » à l'étranger fait partie de la stratégie de Moscou qui vise à renforcer son influence tout en évitant d'apparaître ouvertement en première ligne. Au vu des exactions commises par cette milice sur différents théâtres d'opération, des dirigeants de Wagner, dont Evgueni Prigogine, ont fait l'objet de sanctions de l'Union européenne en octobre 2020, confirmées par la Cour de justice de l'Union européenne en juin 2022, en raison des agissements de la SMP en Libye et en Ukraine. L'Assemblée nationale a pour sa part adopté le 9 mai 2023 une résolution appelant la France et l'Union européenne à inscrire *Wagner* sur la liste des organisations terroristes.

Wagner n'est pas la seule entité privée agissant pour le compte du pouvoir russe. *Convoy*, une nouvelle société militaire privée a vu le jour en Crimée, à la fin de l'année 2022, dans un contexte de frictions sur le théâtre ukrainien entre Wagner et le ministère russe de la Défense.

2. La Chine et sa stratégie du « front uni »

*****

En Chine, où il existe une longue histoire du renseignement et de l'espionnage, les opérations d'influence se sont considérablement intensifiées et durcies ces dernières années avec des méthodes très spécifiques, différentes

des modes opératoires russes, et des effectifs considérables puisque l'équivalent de la DGSE chinoise peut se prévaloir de plus de 250 000 agents.

L'action des autorités chinoises s'étend toujours d'avantage au-delà de l'espionnage au sens strict, ce qui conduit nos services de renseignement à élargir leurs champs d'investigation pour lutter contre tout le spectre des ingérences (politiques, économiques, académiques, médiatiques) portant atteinte aux intérêts fondamentaux de la Nation.

La loi chinoise du 28 juin 2017 sur le renseignement national a largement étendu les pouvoirs des services chinois de renseignement, créant notamment des contraintes légales pour que les citoyens et les entreprises participent à la collecte de renseignement, tant sur le territoire chinois qu'à l'étranger. La loi précise dans son article 7 que « *toute organisation ou citoyen doit soutenir, assister et coopérer avec les activités liées au renseignement national* ». Les articles 12 et 14 indiquent que les services chinois peuvent établir des « *relations coopératives avec les individus et les organisations compétentes* » pour conduire des missions, ainsi que « *demander aux organes, aux organisations et aux citoyens compétents de leur assurer le soutien, l'aide et la coopération nécessaires* ». **Cette disposition fait de tout ressortissant Chinois un potentiel espion**, l'obstruction au travail de renseignement étant par ailleurs passible de sanctions (article 25). Les services de renseignement chinois peuvent ainsi avancer à bas bruit en prenant pour intermédiaires des personnes physiques dites « cooptées » et un maillage associatif communautaire important en France (associations d'étudiants, de commerçants…) regroupant des membres de la diaspora.

L'empire du milieu est entré dans une nouvelle phase où la stratégie d'ingérence occupe une place centrale, autour du concept de **« Front uni »**.

Cette politique conçue et déployée par le **Parti Communiste Chinois** (PCC) consiste à entraver ses ennemis intérieurs comme extérieurs, à contrôler les groupes qui peuvent défier son autorité, à construire une coalition autour du Parti pour servir ses intérêts et à projeter son influence jusqu'à l'étranger. **Le Front uni est une stratégie politique et un réseau d'institutions publiques et privées et d'individus clés, placés sous le contrôle du Parti communiste chinois** (PCC) et utilisés pour faire avancer les intérêts du Parti au sein et à l'extérieur du pays. Avec le Front uni, tout procède du PCC et chacun doit servir cette stratégie : entreprises publiques comme privées, chinois de l'intérieur comme à l'étranger.

C'est ainsi que le parti des 50 centimes (*wumao dang*) fait référence aux commentateurs en ligne engagés par les autorités chinoises pour écrire des articles ou des commentaires favorables au PCC sur les réseaux sociaux, afin de mettre fin aux critiques envers la politique chinoise ou ses dirigeants. Ils

opèrent aussi bien sur l'Internet chinois qu'étranger. Cette appellation du « parti des 50 centimes » provient de l'allégation selon laquelle les commentateurs sont payés 50 centimes de yuan pour chaque publication.

Pour mener à bien sa stratégie de puissance, la Chine utilise différents leviers d'action :

– Le recours aux diasporas qui représentent 40 à 60 millions de personnes dans le monde, dont 600 000 en France. La force du dispositif de renseignement et d'ingérence chinois à l'étranger repose sur l'appui fourni par cette diaspora, notamment dans le cadre de la lutte contre les cinq poisons qui sont autant de menaces pour la stabilité du pouvoir : les démocrates, le Falun Gong, Taïwan, le Tibet et le Xinjiang. *****

– Les médias : le pouvoir Chinois aurait investi 1,3 milliard d'euros par an depuis 2008 pour mieux contrôler son image dans le monde. Les grands médias chinois ont une présence mondiale, dans plusieurs langues et sur tous les réseaux sociaux, y compris ceux bloqués en Chine. Pékin cherche aussi à contrôler les médias sinophones à l'étranger. En France, les médias privés en langue chinoise comme « *Nouvelles d'Europe* », quotidien édité en langue chinoise, sont sous le contrôle du PCC.

– L'économie, à travers des investissements chinois très dynamiques dans des secteurs stratégiques comme l'énergie ou les transports, le rachat d'entreprises et/ ou la prise de participations dans le capital d'entreprises, notamment celles dont la technologie est duale. ***** a permis de documenter un risque concernant les entreprises françaises de biotechnologies avec des transferts potentiels de licences en virologie ou en oncologie, mais également la propension de certains fonds activistes dans le domaine du *Private Equity* et du *Venture Capital* à cibler des ***** ou des PME spécialisées dans les technologies de rupture (calcul quantique, science de la donnée) qui conditionneront la souveraineté numérique de demain.

– Les universités et le monde de la recherche avec comme principal levier la dépendance financière qui peut avoir une influence sur le contenu des cours, le matériel pédagogique ou la programmation d'événements.

– La langue chinoise autour des instituts *Confucius* dont la mission est de promouvoir la langue et la culture chinoises. Mais ces instituts sont avant tout au service d'une stratégie d'influence et du développement d'un narratif positif pour servir les intérêts du parti. Leur implantation au sein des universités et autres établissements d'enseignement supérieur hors de Chine peut leur conférer un effet de levier sur les institutions d'accueil. L'Institut *Confucius* de Lyon, créé en 2009 à l'Université Lyon 3, a ainsi été fermé en 2013 après la nomination d'un directeur Chinois qui exigeait de prendre part à

la définition des contenus pédagogiques et des enseignements diplômant de l'Université.

Au final, les actions d'ingérences chinoises consistent autant à développer un narratif positif sur la Chine qu'à collecter des informations *via* des universités, l'espionnage, la compromission et l'achat de savoir-faire, tout ceci concourant au programme stratégique « *Made in China 2025* » visant notamment au rattrapage technologique du pays.

3. La Turquie et ses velléités d'emprise

Les relations bilatérales franco-turques se sont dégradées ces dernières années du fait notamment de l'offensive turque en octobre 2019 contre les forces kurdes en Syrie, alliées des Occidentaux. L'interventionnisme turc en Libye, en Méditerranée orientale – où un incident a opposé des bâtiments turc et français en juin 2020 – et la politique française contre l'extrémisme islamique ont également creusé les antagonismes entre Paris et Ankara, au point que le Président de la République Emmanuel Macron a lui-même évoqué au printemps 2021 un risque avéré d'ingérence turque lors de l'élection présidentielle de 2022.

Les ingérences turques ont pour but de contrôler la diaspora turque en tant que relai des idées du pouvoir d'Ankara, c'est-à-dire hostiles aux Kurdes et aux Arméniens.

On peut identifier quatre modes opératoires distincts de la Turquie pour promouvoir ses intérêts :

– **Les enseignements langues et culture d'origine (ELCO)**, dispositif mis en place en 1977 dans le but de permettre aux enfants de parents immigrés de conserver un lien avec leur pays d'origine. Les cours sont assurés par des enseignants recrutés, payés et encadrés par les pays d'origine. Or certains enseignants ont pu utiliser ce dispositif pour promouvoir une orientation politique ou défendre des actions contraires aux valeurs de la République. Aussi, depuis 2020, les ELCO ont été systématiquement remplacés par le dispositif des « enseignements internationaux de langue étrangère » (EILE) instauré en 2016 qui met notamment fin à la nomination et à la rémunération des enseignants par des États étrangers.

– **La pratique religieuse** est également un puissant levier pour promouvoir une idéologie politique. À cet égard, le financement de lieux de culte comme le détachement d'imams au sein des mosquées françaises, jusqu'alors autorisé, a permis à la Turquie de peser sur l'Islam de France. ***** sur un nombre total estimé à 2 600 mosquées en France. Le Président de la République a annoncé que la France entendait mettre fin, d'ici à 2024, à cette

pratique des imams détachés. Une mesure qui vise notamment l'influence religieuse de la Turquie qui repose en France sur la *Ditib*, émanation du ministère turc des affaires religieuses, la *Diyanet*. Voix officielle et historique du culte musulman sunnite turc, historiquement modéré, il représente environ 250 associations et 120 imams turcs ou d'origine turque sous le régime de l'imam détaché. Par ailleurs, le *Millî Görüş,* proche des Frères musulmans, est une organisation islamiste qui compte environ 100 000 adhérents sur le territoire européen avec une antenne française, la Confédération islamique *Millî Görüş* (CIMG), dont de plus en plus de voix réclament la dissolution, qui a refusé de signer la charte des principes pour l'Islam de France. Le *Millî Görüş* a dû finalement renoncer à solliciter une subvention municipale pour la construction de la Grande Mosquée de Strasbourg.

– L'entrisme politique *via* la participation aux élections locales et nationales par le biais de listes communautaires et / ou de consignes de votes diffusées sur les réseaux sociaux. Ainsi en Alsace, le parti « égalité et justice » (PEJ), islamo-conservateur est considéré comme une officine officieuse de l'AKP, le parti islamo-conservateur Turc et vise à recueillir des voix parmi la diaspora turque en France. Aux élections législatives de juin 2017, le PEJ a présenté 52 candidats dans 28 départements avec des scores ne lui permettant toutefois pas d'accéder au financement public des partis politiques. Ce parti a été dissous en octobre 2019. Lors des élections législatives de juin 2022, plusieurs candidats ***** se présentant comme indépendants, étaient en réalité engagés au sein de l'association Cojep (Conseil pour la justice, l'égalité et la paix) qui fait valoir en France les intérêts de l'AKP.

– Une présence active sur les réseaux sociaux pour diffuser des messages hostiles en réponse à des orientations politiques comme la loi sur le séparatisme. Des cyberattaques ont également été attribuées à des groupes turcs notamment au lendemain de l'adoption par l'Assemblée nationale d'une proposition de loi condamnant la négation du génocide arménien.

4. L'Iran et sa diplomatie des otages

L'Iran se présente régulièrement comme l'éternelle victime des jeux des puissances étrangères, dénonçant les ingérences étrangères dont elle ferait elle-même l'objet et qui viseraient à déstabiliser le régime. En novembre 2022, le ministre de l'Intérieur iranien, Ahmad Vahidi, a ainsi déclaré que plusieurs agents des services de renseignement français avaient été arrêtés lors des manifestations en cours dans le pays. Cette tendance à associer les maux de l'Iran aux étrangers répond à une histoire marquée par l'ingérence des puissances dans le pays depuis le Grand jeu qui opposa au XIX^{e} siècle les impérialismes britannique et russe en Asie centrale et qui a fondé une méfiance envers les puissances étrangères. L'histoire du pays serait

ainsi celle d'une succession d'ingérences d'acteurs étrangers déterminés à promouvoir leurs intérêts sans tenir compte des conséquences sur l'économie et la société locales.

Les modes opératoires auxquels l'Iran a recours relèvent du registre de **l'action violente**, éloigné du *soft power*. Il s'agit en priorité de neutraliser toute dissidence avec des méthodes comme le kidnapping et / ou l'assassinat. La **« diplomatie des otages »** est également une signature du régime iranien qui procède à l'arrestation de ressortissants de différents pays pour s'en servir comme monnaie d'échange. La libération le 12 mai 2023 de deux otages français, Benjamin Brière et Bernard Phelan, après respectivement trois ans et six mois d'emprisonnement rappelle combien les démocraties se trouvent dans une situation vulnérable face à des régimes autocratiques *****. Devant de telles pratiques, à l'initiative du Canada, une déclaration internationale contre la détention arbitraire dans les relations d'État à État a été adoptée en 2021 et signée par 70 pays.

Parmi les modes opératoires de plus en plus utilisés par l'Iran figurent également les **attaques informatiques**. *****

5. Nos alliés n'agissent pas toujours comme des amis

Lors de son audition, le 2 mai 2023 par la Commission d'enquête parlementaire sur les ingérences étrangères, l'ancien Premier ministre François Fillon a déclaré que le plus grand nombre d'ingérences auxquelles il avait personnellement été confronté émanaient « *d'un pays ami et allié qui s'appelle les États-Unis* ». L'ancien Premier ministre a ajouté que durant son quinquennat à Matignon (2007-2012), il avait été « *écouté avec le président Sarkozy pendant cinq ans par la NSA* », (*National Security Agency*), une agence technique de renseignement américaine.

L'affaire Pegasus a révélé au grand jour, s'il en était besoin, que l'espionnage est une pratique généralisée, y compris entre alliés. Le logiciel espion développé par l'entreprise israélienne NSO Group et fourni à une dizaine de pays du Proche-Orient, d'Afrique, d'Europe et d'Asie a mis en évidence le rôle des autorités israéliennes dans l'autorisation accordée pour exporter ce logiciel.

En matière de renseignement, il y a des alliés, mais pas d'amis bien qu'il existe un pacte de non-espionnage entre les « *five eyes* » que sont les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande.*****

Le renseignement, de par sa nature d'aide à la décision du pouvoir politique est assurément une pratique courante, y compris entre alliés. En

revanche, à la différence des stratégies d'ingérence, le fait de s'espionner entre alliés ne traduit pas une intention hostile comme pourraient l'être des actions de subversion telles que le financement de partis politiques, la corruption, la compromission d'élus et de hauts fonctionnaires ou la manipulation de l'information dans les médias et sur les réseaux sociaux.

Loin d'être seulement lié à des questions de sécurité au sens militaire, l'espionnage concerne le champ économique, et c'est là que nos alliés n'étant pas nos amis, **le concept de souveraineté doit primer sur toute autre considération**.

À cet égard, **l'ingérence par le droit**, à travers l'extraterritorialité des normes, est un trait caractéristique d'une forme de domination des États-Unis qui agissent unilatéralement sur le territoire d'États tiers sur le fondement de leurs lois internes. C'est ainsi que depuis 1976, sur le fondement de la règlementation ITAR (*International Traffic in Arms Regulations*), les États-Unis disposent de la capacité d'interdire mondialement l'export d'armes vers certains pays dès lors qu'un simple composant du produit est d'origine américaine. En vertu de cette loi, les entreprises étrangères ont l'obligation de transmettre des informations sur certains biens sensibles.

Le système ITAR concerne de nombreuses entreprises européennes de défense. L'administration américaine s'en est prévalue pour bloquer en 2018 l'exportation de missiles SCALP et MBDA vers l'Egypte au motif de la présence d'une puce électronique américaine. Au cœur du contrat de vente de 24 *Rafales* supplémentaires pour un montant de deux milliards d'euros, les missiles SCALP ont finalement pu être livrés, mais avec un retard important suite à l'intégration d'un composant analogue par MBDA. *****

De telles réglementations créent des distorsions de concurrence et peuvent contraindre les entreprises concernées à divulguer, sous couvert de légalité, des informations confidentielles. Face à la multiplication des enquêtes d'autorités judiciaires étrangères, sur la base de lois offensives à portée extraterritoriale, à l'encontre d'entreprises françaises commerçant à l'international, le renseignement doit contribuer à identifier, dénoncer, voire entraver les actions malveillantes et les actions d'influence faussant l'environnement juridique et normatif des acteurs économiques.

La création du parquet national financier et de l'Agence française anticorruption puis la loi Sapin II, ont répondu en partie à cette épée de Damoclès dirigée vers nos actifs les plus stratégiques. Pourtant, le risque demeure et il faut être vigilant à ce que certains cabinets de conformité anglo-saxons actifs au sein d'entreprises sensibles ne transfèrent pas hors de France les informations critiques auxquelles ils ont accès.

C. DES VULNÉRABILITÉS PERSISTANTES

D'un point de vue général et intemporel, les principales vulnérabilités demeurent humaines. Les services utilisent l'acronyme « MICE » pour *Money, Intérêt, Corruption et Ego*. Ce sont là des leviers traditionnels de la manipulation, opportunément exploités par des professionnels du renseignement.

1. Notre naïveté

La première des vulnérabilités, c'est la naïveté qui provient d'une méconnaissance du danger. Elle concerne aussi bien les décideurs publics (élus et hauts fonctionnaires) que les entreprises et les milieux académiques.

En 2021, sous l'égide du SGDSN et de la CNRLT, un **plan global de sensibilisation des acteurs publics et privés aux ingérences étrangères** a été mis en place qui a conduit, entre juillet 2021 et juillet 2022, à près de 10 000 actions de sensibilisation qui ont concerné environ 55 000 personnes. La DGSI a par ailleurs procédé à la sensibilisation, en 2022, de l'ensemble des cabinets ministériels. Ces actions visent à participer au développement d'une culture de la sécurité chez les publics destinataires. Elles ont conduit à un accroissement du nombre de signalements de situations inappropriées qui, lorsqu'elles le justifiaient, ont donné lieu à des investigations.

a. La sensibilisation des élus nationaux et locaux

S'agissant des élus, la Délégation parlementaire au renseignement a recommandé à maintes reprises la mise en place de sessions de sensibilisation des députés et des sénateurs aux risques d'ingérences étrangères et aux bonnes pratiques à respecter, en particulier lors des déplacements à l'étranger. À l'initiative des présidents des deux chambres, la DGSI effectue désormais ces sensibilisations qui concernent également les collaborateurs des parlementaires. Des infrastructures de communication sécurisées – messagerie ISIS, lignes téléphoniques sécurisées – ont également été installées, ou sont en voie de l'être, à l'Assemblée nationale et au Sénat.

La sensibilisation des élus locaux au risque d'ingérence reste en revanche très imparfaite. Or les collectivités territoriales sont susceptibles d'accueillir des investissements étrangers pouvant constituer le support d'une éventuelle ingérence étrangère. De même, en matière de commande publique, la préférence accordée aux moins disant peut emporter des risques réels d'ingérences étrangères. Or les règles des marchés publics ne laissent généralement pas ou peu de marges manœuvres aux décideurs locaux pour écarter des entreprises dont le profil présente un risque potentiel pour la protection des intérêts fondamentaux de la Nation. Les liens qui peuvent

exister entre des associations locales et certains pays nécessitent également une vigilance accrue de la part des élus, notamment au regard du risque de séparatisme et d'atteinte aux valeurs de la République. La **double nationalité constitue à cet égard une vulnérabilité** que les acteurs de l'ingérence ne manquent pas d'exploiter. Dès lors, si la détention de la double nationalité n'empêche en rien l'expression d'une loyauté pérenne, il convient néanmoins d'opérer une mise en garde, *a minima* une sensibilisation au profit des intéressés.

Au vu de l'intensification de la menace et des responsabilités qui pèsent sur les élus locaux, la Délégation parlementaire au renseignement recommande que soit organisé dans chaque département, à l'initiative du Préfet et en lien avec les services territoriaux de sécurité intérieure, une session de sensibilisation des élus locaux aux risques d'ingérences au lendemain de chaque élection locale (municipale, départementale et régionale). **(Recommandation n° 5)**

b. La sensibilisation des entreprises

La sécurité économique est un impératif stratégique qui nécessite une appropriation collective de l'ensemble des acteurs qui y concourent, et pas seulement des pouvoirs publics. La sensibilisation des acteurs économiques, à chacun des maillons de la vie de l'entreprise, est requise pour réduire les risques extra-financiers pesant sur l'entreprise comme la non-conformité, le risque de réputation, de fuites de données stratégiques ou encore d'usage du numérique à des fins malveillantes.

Si les grands groupes sont bien outillés juridiquement et techniquement pour prévenir au mieux les tentatives d'ingérences étrangères, beaucoup reste à faire pour les plus petites structures, TPE/ PME /ETI et les start-up confrontées à des tentatives de déstabilisation et d'espionnage par la captation de données par des acteurs étrangers.

Des outils ont été conçus ces dernières années, tant par le Service de l'information stratégique et de la sécurité économique (SISSE) à Bercy que par la DGSI pour apporter aux acteurs économiques un mode d'emploi très opérationnel sur la sécurité des entreprises et la protection de leurs informations stratégiques.

Pour réduire les vulnérabilités, les préconisations sont d'ordre organisationnel (à destination des managers), technique (à destination des responsables de la sécurité des systèmes d'information, des locaux ou de la logistique, mais aussi potentiellement à chaque employé dans son comportement quotidien) et comportemental.

Les deux services menants (DGSI et DRSD) dans le domaine de la protection économique ont effectué en 2022 plus de 700 conférences au profit des dirigeants et salariés des *****.

c. La sensibilisation du monde académique

Deux rapports récents ont attiré l'attention sur la vulnérabilité du monde académique et son ciblage par des puissances étrangères. Le premier, spécifique à l'enseignement supérieur et à la recherche (ESR), est celui du sénateur André Gattolin, issu des travaux de la mission d'information sénatoriale sur « *les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences* (1) ». Le second est un rapport de l'IRSEM sur « *Les opérations d'influence chinoises, un moment machiavélien* » de MM. Charon et Jeangène Vilmer qui, comme son titre le laisse entendre, s'attache à démontrer des influences chinoises, notamment dans l'enseignement supérieur et la recherche.

Les vulnérabilités du monde académique français résultent **de la conjugaison de plusieurs facteurs** que sont une insuffisance de ressources budgétaires, des modalités de gouvernance peu adaptées à la prise en compte du risque d'ingérence – plus précisément dans cette zone grise qui s'étend de l'influence à l'ingérence – et la culture d'une recherche ouverte fondée sur le partage des connaissances et la circulation des idées.

Dans ce contexte, les tentatives de pénétration du milieu universitaire français sont initiées par le biais de plusieurs vecteurs. Certaines puissances étrangères mènent leurs opérations d'influence directement depuis leurs emprises diplomatiques dans le but de cultiver un réseau d'universitaires qui leur soit favorable. D'autres privilégient l'utilisation de chercheurs et doctorants comme agents d'influence au sein des universités françaises.

Toutefois, le principal vecteur de pénétration demeure les coopérations avec les universités étrangères. En effet, nos institutions académiques se révèlent de plus en plus dépendantes de financements étrangers, notamment chinois, ce qui emporte des conséquences sur leur liberté académique.

La DGSI, en étroite coordination avec le ministère de l'enseignement supérieur et de la recherche, a élaboré à l'été 2021 un plan d'action dédié au renforcement et au suivi des structures et organismes de recherche les plus stratégiques. Décliné en plusieurs actions, ce plan vise principalement à :

---

(1) « Mieux protéger notre patrimoine scientifique et nos libertés académiques » - Rapport d'information d'André Gattolin, fait au nom de la mission d'information du Sénat sur les influences étatiques extra-européennes : (septembre 2021).

– Renforcer le travail de sensibilisation effectué auprès de la communauté scientifique, notamment auprès de directeurs d'unités, de chercheurs et d'experts.

– Délivrer un discours efficace auprès du milieu de la recherche et diversifier les points de contacts du Service en s'appuyant sur les outils pédagogiques visant à expliquer l'action du Service au profit du monde de la recherche.

La ministre de l'enseignement supérieur et de la recherche, Sylvie Retailleau, a fait de ce sujet une des priorités de son ministère, en lien avec la communauté du renseignement.

La DGSI a ainsi rencontré les directeurs et présidents des principaux organismes de recherche et grandes écoles françaises (Inria, Cnes, CEA, CNRS, Inserm, Institut PASTEUR, Sciences Po, ESCP, Mines, etc.). Ces échanges ont permis d'identifier les spécificités de ce secteur : logique de coopération avec l'étranger, publications internationales, enjeu du financement.

Par ailleurs, le suivi des structures sensibles a été renforcé : 300 contacts auprès des établissements d'enseignement supérieur et de recherche ont été réalisés au premier semestre 2022 (autant que sur l'ensemble de l'année 2021). *****

2. L'insuffisant niveau de sécurité des systèmes d'information, publics comme privés

Au-delà des vulnérabilités humaines, le niveau de sécurité des systèmes d'information, publics comme privés, se révèle encore, à bien des égards, perfectible au vu de l'utilisation fréquente de systèmes obsolètes ou en voie d'obsolescence, d'absence de correctifs de sécurité à jour, de recours à des protocoles de communication non sécurisés, etc. La sensibilisation fait régulièrement défaut, quand les entreprises n'ont tout simplement pas de chaîne SSI clairement identifiée en leur sein. Ceci est d'autant plus important que l'aspect humain est une composante essentielle dans les cyberattaques observées : l'ouverture d'un courriel d'hameçonnage par un salarié reste efficace pour déjouer les meilleurs dispositifs de sécurité.

Dès lors que les victimes sont compromises, on peut aussi faire le constat d'un manque de moyens et de mesures de sécurité suffisants pour les investigations techniques voire pour la remédiation. La DGSI relève un enjeu majeur concernant les infrastructures d'attaque de très grande taille, pouvant être composées de plusieurs milliers d'équipements compromis à travers le monde, chaque équipement pouvant n'être utilisé individuellement que

quelques jours par l'attaquant. Ces caractéristiques rendent ces réseaux particulièrement complexes à suivre et imposent une très grande réactivité aux services.

3. Les difficultés d'accès au financement des entreprises

Les prises de contrôle capitalistiques étrangères au sein des entreprises, start-up et laboratoires stratégiques ne sont pas sans conséquences. Le risque existe tant pour les entreprises concernées que pour l'État, au vu des enjeux en termes de souveraineté. **Cela concerne en particulier les entreprises duales** au regard des enjeux en matière de sécurité et de défense.

Il est fréquent qu'une entreprise incubée en France n'ait d'autre choix que de se tourner vers un investisseur étranger pour changer d'échelle. Le basculement du capital de start-up stratégiques à l'occasion d'une levée de fonds peut certes être **une chance pour l'entreprise concernée mais aussi une vulnérabilité pour la souveraineté nationale**. Le fait qu'une start-up stratégique ne trouve aucun – ou du moins pas suffisamment – de financements en France ou en Europe et se tourne vers des fonds étrangers peut emporter d'importantes conséquences. Dans son flash de janvier 2022 sur l'ingérence économique et les risques liés aux investisseurs étrangers déloyaux, la DGSI met particulièrement en garde sur la vulnérabilité financière de start-up françaises développant des technologies stratégiques. Dans les secteurs de la medtech et de la biotech, on estime en effet à 80 % le pourcentage de jeunes pousses françaises rachetées, *in fine*, par de grands groupes américains.

Nos PME ont besoin d'investisseurs pour croître ; à défaut de financements bancaires qu'elles ne parviennent à obtenir, elles deviennent la proie d'investisseurs étrangers pas toujours bienveillants. En effet, un fonds d'investissement activiste peut, en ne possédant que quelques pourcents du capital de l'entreprise, déclencher une campagne de déstabilisation.

La contre-ingérence doit permettre d'articuler les objectifs de sécurité économique au service de la lutte contre les risques d'ingérences d'États tiers avec la nécessité de préserver l'accès au financement des entreprises françaises innovantes qui conditionnent la souveraineté industrielle et numérique de demain.

Des outils juridiques existent pour bloquer certains investissements étrangers, notamment l'article L. 151-3 du code monétaire et financier qui soumet ceux-ci à une procédure d'autorisation préalable « *dans le cas où ils pourraient nuire aux intérêts du pays* ».

En 2022, s'agissant des investissements étrangers en France, 325 opérations ont été examinées (contre 328 en 2021) et 131 d'entre elles ont été autorisées dont plus de la moitié (53 %) sous condition.

Afin de se prémunir de prises de participations opportunistes non européennes pouvant présenter des menaces pour la sécurité nationale, **le seuil déclenchant le contrôle des IEF dans les sociétés françaises cotées a été abaissé au printemps 2020 dans le contexte de la crise sanitaire, de 25 % à 10 % des droits de vote**. Cette mesure a été prolongée jusqu'au 31 décembre 2023.

Le renseignement prend toute sa part à l'évaluation des risques et à l'accompagnement des entreprises ciblées par des investisseurs étrangers pouvant nuire aux intérêts du pays. À titre d'exemple, *****

Il est ainsi nécessaire d'activer une multiplicité de leviers pour éviter que des entreprises stratégiques ne passent sous contrôle étranger hostile du fait d'une faiblesse d'accès aux financements. Dans ce contexte, la Délégation parlementaire au renseignement estime nécessaire de **pérenniser à 10 % (au lieu de 25 %) le seuil de déclenchement de la procédure de contrôle des IEF non européens**. **(Recommandation n° 6)**

4. Nos valeurs démocratiques : notre force et notre faiblesse

Les démocraties sont par leur nature même vulnérables face aux moyens utilisés par des régimes autoritaires dont les méthodes relèvent d'un autre registre.

Dans sa résolution adoptée le 9 mars 2022 sur « *l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation* », le Parlement européen se déclare ainsi « *préoccupé du manque criant de sensibilisation, y compris parmi le grand public et les représentants des pouvoirs publics, à la gravité des menaces actuelles que présentent les régimes autoritaires étrangers et d'autres acteurs malveillants et qui visent tous les niveaux et secteurs de la société européenne dans le but de nuire aux droits fondamentaux et à la légitimité des autorités publiques, d'exacerber la fragmentation politique et sociale et, dans certains cas, même de mettre en danger la vie des citoyens de l'Union* »

Comme l'a déclaré Bernard Emié, directeur général de la sécurité extérieure, le 15 février 2023 devant la Commission d'enquête parlementaire sur les ingérences étrangères : « *Nous avons le privilège d'être des démocraties, ce qui impose aux services de renseignement de nombreuses limitations : des cadres légaux, des contrôles de méthodes propres aux démocraties* ».

La force de la démocratie a donc pour contrepartie une vulnérabilité qui doit conduire à **développer des outils de lutte contre les ingérences étrangères qui demeurent compatibles avec les valeurs d'un système démocratique** que sont notamment la liberté d'expression, le pluralisme des médias, la libre concurrence, la transparence, la protection des données personnelles, etc.

Le sujet est double : il s'agit tout à la fois de se défendre face à des pratiques qui ont pour visée de saper le bon fonctionnement de notre démocratie et dans le même temps de développer des outils de contre-ingérence qui soient compatibles avec le respect de nos valeurs démocratiques.

C'est à l'échelle européenne que se situent aussi les enjeux. Alors que le Parlement européen conduit des travaux approfondis que le sujet des ingérences étrangères dans le cadre d'une commission spéciale, la Commission européenne plaide en faveur d'une législation européenne contre les ingérences qui pourrait prendre la forme d'un **paquet législatif et règlementaire** « **défense de la démocratie européenne** ». Il s'agit d'introduire des normes communes de transparence et de responsabilité pour les services de représentation d'intérêts qui seraient payés ou commandités depuis l'extérieur de l'Union européenne, afin de contribuer au bon fonctionnement du marché intérieur et de protéger la sphère démocratique de l'Union contre les ingérences extérieures dissimulées.

Pourtant, cette proposition de la Commission européenne est loin de faire l'unanimité. Dans une lettre ouverte à sa Présidente Ursula Von der Leyen, **230 organisations de la société civile ont mis en garde contre le risque que ce futur texte contrevienne au droit international et européen en matière de droits de l'Homme** et en particulier à l'exercice des libertés civiques, la liberté d'association et la liberté d'expression. Les signataires rappellent que « *plusieurs États membres de l'UE ont déjà adopté ou proposé des législations et des politiques qui restreignent volontairement ou involontairement l'espace civique, ce qui a donné lieu à des protestations et contestations tout ce qu'il y a de plus justifié* ».

Pour toutes ces raisons, et compte tenu de l'évolution permanente des menaces qui pèsent sur la sécurité nationale, de leur intensification et de la nécessité de sensibiliser l'ensemble des acteurs publics et privés pour s'en prémunir, la Délégation parlementaire au renseignement considère important que ces sujets n'échappent pas au débat public. Aussi recommande-t-elle, comme c'est le cas dans la plupart des démocraties occidentales, qu'un **rapport public au Parlement soit établi chaque année par le Gouvernement sur l'état des menaces pesant sur la sécurité nationale** et

que ce rapport fasse l'objet d'un débat sans vote au Parlement **(Recommandation n° 7)**.

II. LA NOUVELLE PRIORITÉ DONNÉE À LA CONTRE-INGÉRENCE OUVRE UN NOUVEAU CYCLE DU RENSEIGNEMENT

Le climat de guerre froide est de retour et avec lui, les pratiques qui lui étaient caractéristiques. En matière de renseignement, nous assistons au chevauchement de deux cycles entre celui lié à la lutte contre le djihadisme – marqué par une coopération des grandes puissances et de leurs services de renseignement – et celui de la confrontation qui bouleverse les équilibres du monde.

A. UN CHANGEMENT DE PARADIGME POUR LA COMMUNAUTÉ DU RENSEIGNEMENT

Depuis une quinzaine d'années, plusieurs documents sont venus prendre acte d'un changement de paradigme pour la communauté du renseignement.

1. La redéfinition des priorités stratégiques du renseignement au vu du contexte nouveau

Déjà en 2008, le **Livre blanc sur la défense et la sécurité nationale** dressait le constat que « *la poursuite des échanges mondialisés et le développement de nouveaux pôles de puissance sont propices à des activités de renseignement offensif visant la France et l'Europe, comme au développement de stratégies d'influence destinées à amoindrir notre rôle dans le monde et sur le marché international* ». Et de poursuivre que « *les éléments qui garantissent la supériorité technologique comme notre patrimoine scientifique, économique et militaire continueront à faire l'objet de manœuvres extérieures. Ces manœuvres viseront à obtenir des informations protégées ou secrètes sur notre stratégie de sécurité, notre diplomatie, nos technologies civiles et militaires et la stratégie de nos entreprises* ».

Le Livre blanc alertait sur nos vulnérabilités soulignant que « *les actions étrangères privilégieront les attaques informatiques. Dans d'autres cas, elles peuvent viser l'affaiblissement d'une entreprise ou une personne, par une désinformation générale propagée sur les médias et via Internet. Pourront aussi être visées par de telles actions les communautés françaises à l'étranger et les communautés étrangères en France* ».

Et de conclure que « *ces risques imposent à la France et à l'Europe de développer les capacités de leurs services de contre-ingérence, mais aussi les moyens de la « puissance douce » (soft power), reposant notamment sur la présence dans les médias et sur Internet, la culture d'entreprise et sur la*

sensibilisation préalable des hauts responsables du secteur privé et du secteur public ».

Cinq ans plus tard, le **Livre blanc « sécurité et défense » de 2013** soulignait la montée en puissance des nouveaux champs de confrontation au premier rang desquels le cyber et l'espace : « *Le cyberespace est donc désormais un champ de confrontation à part entière. La possibilité, envisagée par le précédent Livre blanc, d'une attaque informatique majeure contre les systèmes d'information nationaux dans un scénario de guerre informatique constitue, pour la France et ses partenaires européens, une menace de première importance. L'espace extra-atmosphérique est devenu indispensable au fonctionnement de services essentiels. Dans le domaine militaire, le libre accès et l'utilisation de l'espace sont des conditions de notre autonomie stratégique. Ils rendent possible le maintien et le développement de capacités technologiques dont dépendent la qualité de notre outil de défense et, en particulier, la crédibilité de notre dissuasion nucléaire* ».

*****

La **stratégie nationale du renseignement** publiée en juillet 2019 reprend ces analyses à son compte, considérant que « *l'ingérence et l'espionnage auxquels se livrent plusieurs puissances étrangères de manière décomplexée entraînent des préjudices majeurs pour nos intérêts (politiques, stratégiques, scientifiques…), notre souveraineté et ceux de nos partenaires européens. Compte tenu de sa politique volontariste et attractive de recherche et de développement, comme d'une insuffisante culture de la sécurité dans les milieux concernés, la France constitue une cible privilégiée pour des puissances ou des structures étrangères qui cherchent à s'approprier nos savoir-faire et nos résultats. Parmi les formes préoccupantes d'ingérences, notons l'acuité et la sophistication des actions de manipulation de l'information, tout particulièrement celles orchestrées par des puissances étrangères hostiles à nos intérêts* ».

La stratégie nationale du renseignement assigne ainsi aux services de renseignement la mission *« d'identifier les entités et services agressifs à notre encontre ainsi que leurs cibles, et de décrire leurs buts et leurs méthodes* ». Il s'agit également « *d'en évaluer les conséquences pour notre souveraineté et nos intérêts, afin d'éclairer la décision politique de réponse à ces agissements hostiles* ».

***** la Délégation préconise une prise en compte par le PNOR de ces nouveaux enjeux, en cohérence avec la nouvelle **revue nationale stratégique** adoptée fin 2022, c'est-à-dire après le déclenchement de la guerre en Ukraine, et qui fixe notamment comme objectif stratégique d'assurer notre

capacité à nous défendre et à agir dans les champs hybrides. **(Recommandation n° 8)**

2. De nouvelles façons de travailler

Le retour de la menace étatique et le déploiement de nouvelles formes d'agression ouvrent un nouveau chapitre dans le cycle du renseignement. Dans son discours de vœux aux armées du 20 janvier 2023, le Président de la République a ainsi déclaré que « *le cœur de souveraineté, c'est aussi le renforcement des postures permanentes. Cela suppose des capacités accrues de renseignement qui nous permettent d'anticiper les crises ou les menaces* ».

À la menace terroriste qui demeure élevée, vient désormais s'ajouter une menace permanente et structurelle liée au retour de la compétition entre les États dans un contexte de confrontation des modèles et des valeurs.

Cela n'est pas sans conséquences sur le fonctionnement des services de renseignement si l'on considère que les métiers du renseignement diffèrent en fonction des menaces, comme le contre-espionnage se distingue par exemple du contre-terrorisme. Le contre-terrorisme appelle réactivité, fluidité et adaptation. Travailler contre l'appareil étatique d'un pays comme la Russie ou la Chine requiert une approche, des techniques, des alliances différentes, un *tempo* opérationnel, des mécanismes de protection différents.

S'agissant des coopérations internationales, nous sortons d'une union sacrée face au terrorisme transnational djihadiste, marqué par l'augmentation sensible du nombre et de la densité des coopérations internationales. Devant la nécessité et l'urgence, les services occidentaux ont été conduits à travailler avec des services d'États qui n'étaient pas des partenaires naturels dans le contexte de la guerre froide, et pour certains d'entre eux peu respectueux des droits de l'homme. C'était là un choix assumé par les autorités politiques.

Ce nouveau cycle du renseignement se traduit par plusieurs faits marquants :

D'abord de **nouvelles organisations internes** pour différents services avec la volonté d'adapter leur structure à l'évolution de la menace. L'exemple le plus emblématique est celui de la DGSE avec une **modernisation du Service autour de la création de sept « centres de mission »** : *****. Cette nouvelle organisation interne, plus horizontale et transversale, vise à casser la logique de silos et à raccourcir la chaîne hiérarchique. Concrètement, le rôle des centres de mission en matière de pilotage des actions et des opérations de contre-ingérence est renforcé et affermi, chaque centre de mission étant à la fois l'intégrateur de l'ensemble des dimensions contre-ingérence (cyber, lutte contre les manipulations de l'information, contre-espionnage…) dans son

domaine géographique ou thématique. Cette intégration, notamment au niveau opérationnel, est le gage d'une réactivité accrue.

D'autres services de renseignement ont également adapté leur organisation interne pour tenir compte de l'évolution de la menace. *****

Tracfin a pour sa part fait le choix *****. Ces unités mobilisent expertise et capacité de réponse pénale contre ces menaces, et sont identifiées par les partenaires des autres services et institutions comme les interlocuteurs experts au sein du service.

Les nouvelles façons de travailler des services supposent également le **renforcement des capacités techniques des services de renseignement**. **La loi de programmation militaire (LPM) 2024-2030 fait du renforcement des capacités techniques un objectif stratégique**. Sur les cinq milliards d'euros inscrits dans la LPM, *****. Alors que les sauts technologiques actuels sont de plus en plus rapides, au point de menacer notre autonomie, la France doit renouveler ses capacités d'exploitation et industrialiser ses outils d'investigation numérique. Il s'agit de comprendre des situations sans avoir à dépendre de nos partenaires. Cette capacité à se saisir des sauts technologiques relève donc d'enjeux de souveraineté. Pour ce faire, la France peut s'appuyer sur son aptitude à développer de nouvelles capacités, notamment dans le domaine cyber, tout en couvrant le champ des technologies de rupture. Elle peut aussi compter sur l'acquisition de nouveaux équipements que sont les satellites de renseignement optique et électromagnétique ou encore les avions d'interception électromagnétique Archange.

Enfin, le **développement des partenariats internationaux** ciblés représente une orientation majeure dans la lutte contre les ingérences étrangères. Au-delà des échanges d'analyse sur un état partagé de la menace, ces coopérations internationales sont essentielles, notamment en matière opérationnelle. La DGSI échange ainsi avec nombre de partenaires étrangers, constitués de différents services de sécurité intérieure et extérieure, majoritairement occidentaux. *****

Le renseignement s'impose également plus que jamais comme une **priorité budgétaire** pour les années à venir, avec cinq milliards d'euros prévus dans la nouvelle loi de programmation militaire. Cela va permettre, sur une période decinq ans, le doublement des budgets des trois services de renseignement placés sous l'autorité du ministère des Armées et l'augmentation de leurs effectifs. Cela confirme la montée en puissance de la DRSD qui avait perdu en moyens et en effectifs au cours de la décennie précédente. Il en est de même pour la direction du renseignement militaire (DRM). En termes d'effectifs, il y avait en 2012, 7 700 ETP au sein les

services de renseignement du ministère des armées ; il y en aura plus de 10 000 en 2030. Le budget annuel cumulé des trois services passera de 500 millions d'euros annuels en 2017 à près de 1 milliard d'euros à la fin de la période de la LPM.

*****

B. UNE GOUVERNANCE ADAPTÉE ET MODERNISÉE POUR RÉPONDRE AUX DÉFIS POSÉS PAR LES INGÉRENCES ÉTRANGÈRES

1. La répartition des rôles au sein de la communauté du renseignement

Au sein de la communauté du renseignement, la mission de contre-ingérence relève principalement de trois services (la DGSI, la DGSE et la DRSD) qui peuvent également mobiliser d'autres services et structures dans l'exercice de leurs compétences.

a. Les trois services compétents en matière de contre-espionnage et de contre-ingérence

Les services de renseignement compétents en matière de lutte contre les ingérences étrangères sont **la DGSI** qualifiée de chef de file national, **la DGSE** pour l'action extérieure et **la DRSD** s'agissant de la protection du secteur de la défense.

Le décret du 30 avril 2014 portant création de la **DGSI** énonce que le service « *assure la prévention et concourt à la répression de toute forme d'ingérence étrangère* », ce qui constitue sa première mission. Ce même décret ajoute qu'elle « *concourt à la prévention et à la répression des actes portant atteinte au secret de la défense nationale ou à ceux portant atteinte au potentiel économique, industriel ou scientifique du pays* ».

La DGSI bénéficie d'une compétence exclusive en matière de contre-espionnage, en renseignement et en judiciaire, sur l'ensemble du territoire national. Cette compétence est multiforme : en prévention, en analyse et en entrave, y compris pour entreprendre des actions offensives. Cette compétence concerne aussi des actions menées contre des intérêts de pays tiers, pour lesquels la France est utilisée comme un pays « rebond ». La DGSI se coordonne ainsi avec la DGSE avant toute action extérieure du territoire national pour assurer un suivi pertinent de la mission.

En matière d'ingérences étrangères, au-delà de sa fonction première et historique de contre-espionnage, **la DGSI intervient au titre de la protection**

économique et pour ce qui relève de la lutte contre la manipulation de l'information, elle exerce sa mission à la confluence de l'ingérence étrangère et de la cyberdéfense. L'alinéa 8 du décret de 2014 énonce en effet qu'elle « *concourt à la prévention et à la répression de la criminalité liée aux technologies de l'information et de la communication* », notamment si ces attaques cyber portent atteinte à nos intérêts fondamentaux.

Depuis la création de la DGSI en 2014, la lutte contre les ingérences étrangères n'a cessé de prendre de l'importance. L'action du service s'articule avec l'ensemble des services de l'État concourant à la sécurité nationale et conformément à l'article 3 du décret du 30 avril 2014 : « *Les services concourant à la sécurité nationale transmettent sans délai à la direction générale de la sécurité intérieure les renseignements se rapportant aux activités mentionnées à l'article 2* ».

La DGSI est confrontée à une menace croissante allant de l'espionnage à l'ingérence, la conduisant à évoluer dans ses modes d'appréhension, ces menaces étant principalement portées par deux « puissances conquérantes » que sont la Chine et la Russie, suivie par la Turquie et une République islamique d'Iran qui n'a pas cessé de recourir à un terrorisme d'État, directement ou *via* des intermédiaires. Par ailleurs, le Service porte une attention particulière aux menaces engendrées depuis le Maghreb et l'Afrique subsaharienne, la présence sur notre sol d'importantes communautés originaires de ces zones constituant un facteur démultiplicateur de risques.

Hors des frontières nationales, la mission de contre-espionnage et de contre-ingérence relève exclusivement de la DGSE qui agit au titre de la protection intérêts français à l'étranger. Le Service contribue à l'anticipation, à la détection, à la caractérisation et à l'imputation de manœuvres adverses, dans tous les champs possibles de l'ingérence (cyber, lutte informationnelle, protection de la souveraineté économique, contre-espionnage). **Les missions de contre-espionnage et de contre-ingérence sont de plus en plus intégrées et coordonnées entre la DGSE et la DGSI** pour assurer la continuité de l'action de renseignement. ***** Ainsi, en matière de contre-espionnage, un partenariat étroit a été bâti entre la DGSE et la DGSI, par le biais d'échanges réguliers sur les dossiers en cours et d'actions communes permettant l'instruction d'entraves administratives ou opérationnelles.

*****

LE CONTRE-ESPIONNAGE ET LA CONTRE-INGÉRENCE,
CŒUR DE MÉTIER HISTORIQUE DU RENSEIGNEMENT INTÉRIEUR

Dès la fin du XIX[e] siècle, après l'affaire Dreyfus, les missions de surveillance du territoire qui étaient auparavant sous la responsabilité des armées, sont confiées au ministère de l'Intérieur. D'abord de faible envergure, elles sont structurées et renforcées par la création du contrôle général de la surveillance du territoire (CGST) au sein de la Direction générale de la sûreté nationale en 1934. Dès lors, celui-ci a « *pour mission exclusive d'assurer en France, par une coordination méthodique des attributions de la police spéciale, l'application de la loi du 26 janvier 1934 tendant à réprimer l'espionnage, ainsi que les crimes et délits intéressant la sûreté extérieure de l'État* ».

Mais le CGST durera peu. En effet, les années de guerre voient d'une part la dissolution du service par les autorités allemandes, d'autre part le déploiement de nouvelles approches de collecte du renseignement opérées depuis Londres, puis Alger, par le Bureau central de renseignements et d'action (BCRA) et la Direction générale des services spéciaux (DGSS).

À la Libération, le Général de Gaulle décide de capitaliser sur les nouveaux savoir-faire en matière de contre-espionnage. Le 16 novembre 1944, la Direction de la Surveillance du Territoire (DST) est créée par ordonnance et rattachée à la Direction générale de la sûreté nationale, dépendante du ministère de l'Intérieur.

Au cours de ses premières années d'existence, le Service s'est concentré sur le démantèlement des réseaux allemands, avec l'opération « Liqui » visant à « liquider » et neutraliser les réseaux laissés derrière lui par l'occupant. C'est à cette période que le service a connu le plus grand nombre de morts.

À la fin des années 40, le service a commencé à s'occuper des réseaux russes avant que dans les années 50 et 60, il se concentre davantage sur le FLN et l'OAS dans le contexte de la décolonisation. Au milieu des années 60, la DST s'affirme comme un véritable service de contre-espionnage avec en ligne de mire la principale menace de l'époque que représentait le bloc soviétique, tandis qu'au cours des années 70, les activistes palestiniens et les mouvements de contestation nationale sont dans le viseur des services de renseignement.

C'est au cours des années 90 que la lutte contre le terrorisme islamiste relègue au second plan l'activité de contre-espionnage. Pour autant, le service a toujours veillé à conserver des capacités significatives de contre-espionnage et la création de la DGSI en 2014 est allée dans ce sens. ***** Actuellement, les priorités sont dirigées vers les puissances étrangères que sont la Chine, la Russie, l'Iran et la Turquie. Parmi elles, la menace russe est significativement la plus importante mais à moyen terme, à échéance de dix ans environ, la menace chinoise, globale et systémique, sera assurément la première.

*****

D'une façon générale, *****.

La **DRSD** intervient quant à elle en service de renseignement compétent pour ce qui relève des **vulnérabilités et menaces pensant sur le secteur de la défense** (personnel, matériel, informations, entreprises de la

BITD et emprises immobilières). L'action de ce service se décline dans trois domaines :

– La **contre-ingérence des forces**, qui s'intéresse à la protection des personnels militaires et civils de la défense, à leur environnement et aux menaces susceptibles de peser sur eux.

– La **contre-ingérence économique** qui vise à protéger la technologie des entreprises françaises du secteur de la défense et à préserver leur compétitivité. À ce titre, la DRSD accompagne plus de 4 000 entités de la BITD.

– La **contre-ingérence cyber** qui consiste à identifier les menaces et les vulnérabilités susceptibles de porter atteinte aux personnes, aux matériels et aux informations sensibles en lien avec le ministère des Armées. Le service contribue à la lutte informatique en participant à la protection des systèmes d'information du ministère et de la BITD. Ses actions ont un caractère autant préventif (sensibilisations, inspections, alertes) que curatif (analyse des cyber-attaques, soutien à la remédiation et accompagnement de la reprise d'activité).

*****

La répartition des compétences entre les services est opérée en fonction de la nature civile ou militaire des entités concernées. *****

Pour mener à bien leur mission de contre-ingérence, les services « menants » peuvent s'appuyer sur l'apport d'autres services de la communauté du renseignement qui par leurs domaines d'intervention et leur expertise technique contribuent à caractériser et à entraver des actions d'ingérence.

i. <u>Les signaux faibles mais fiables de Tracfin</u>

Tracfin soutient les services de renseignement dans la lutte contre les ingérences étrangères en apportant son concours ***** .

En matière de lutte contre les ingérences étrangères, Tracfin fonde son action sur deux corpus juridiques :

– Le code monétaire et financier (CMF), qui définit les pouvoirs de Tracfin en tant que cellule de renseignement financier (CRF) indépendante et automne sur le plan opérationnel, conformément aux recommandations du GAFI et aux directives européennes.

– Le code de la sécurité intérieure (CSI), qui confère à Tracfin, en tant que service de renseignement du premier cercle, des pouvoirs d'investigation

pour assurer la défense et la promotion des intérêts fondamentaux de la Nation.

À ce double titre, le Service dispose de moyens étendus de détection grâce au renseignement financier obtenu *via* les déclarations de soupçons des professions assujetties, les réponses aux droits de communication exercé par le Service et les échanges d'information avec les CRF étrangères. Il recourt également aux techniques de renseignement.

Tracfin joue ainsi un rôle important s'agissant du volet financier des actions d'ingérence. Le service de renseignement rattaché à Bercy, par ses capacités de détection de vecteurs financiers, est ainsi susceptible d'identifier les vecteurs financiers qui rétribuent des entités relais de l'influence d'États tiers, afin d'infléchir les processus de décision nationaux.*****

En matière **d'ingérences économiques**, Tracfin collabore particulièrement avec les autres services menants sur la thématique du renseignement économique, à savoir la DGSI, la DRSD et la DGSE pour protéger la souveraineté économique nationale. Tracfin identifie, alerte et entrave les tentatives de captation de données stratégiques qui découlent de procédures contentieuses parfois instrumentalisées par d'autres acteurs. ***** Des réunions de travail bilatérales, voire multilatérales, peuvent être organisées sur les dossiers qui le requièrent. Du fait de son appartenance au ministère de l'Économie, des finances et de la Souveraineté industrielle et numérique, Tracfin échange également de l'information avec les acteurs de la sécurité économique au sein du ministère et notamment les cabinets des ministres, la direction générale du Trésor, la direction générale des entreprises et le SISSE. Tracfin peut aussi contribuer ponctuellement aux initiatives d'autres ministères (Intérieur, culture) en matière de contre-ingérence.

Tracfin joue également un rôle important s'agissant de la **contre-ingérence dite cultuelle** en détectant le financement étranger de lieux de culte. En 2021, Tracfin a reçu plus de 700 signalements en lien avec des soupçons de financement du terrorisme ou de radicalisation impliquant des structures associatives. Près de la moitié ont concerné le financement d'associations cultuelles, dont l'objet déclaré était la gestion ou la construction de lieux de culte. Les investigations de Tracfin ont mis en exergue une tendance à la dissimulation des fonds perçus par des réseaux associatifs cultuels, celle-ci se matérialisant soit par des montages financiers complexes soit par le non-respect des obligations de transparence comptable. **Les circuits de financement observés par Tracfin confirment les risques d'ingérence de puissances étrangères par le biais de structures associatives promotrices d'une idéologie radicale**. Dans son rapport annuel

2021, le Service indiquait que ces dernières pouvaient être financées directement au moyen de dotations et de virements provenant des organes officiels des États impliqués ou par des rebonds *via* des pays tiers. Si des actions diplomatiques, complétées par la loi « séparatisme » du 24 août 2021 confortant le respect des principes de la République (CRPR) ont mis fin à la plupart des ingérences de nature étatique en provenance *****.

ii. L'apport du renseignement douanier

La DNRED, service de renseignement douanier, concourt également à la contre-ingérence étrangère bien que cette notion d'ingérence ne figure pas, en tant que telle, comme délit ou comme crime, dans le code des douanes. La DNRED lutte davantage contre les prédations que directement contre les ingérences. *****

Comme administration de la frontière et des flux transfrontaliers, les douanes observent ainsi régulièrement au cours de leurs actions des liens avec l'étranger. **À travers l'action du renseignement douanier, cinq domaines peuvent révéler des phénomènes d'ingérences étrangères** :

– Le **contrôle des exportations et le transfert de technologies** : la législation encadre l'exportation des biens dits « à double usage » ; exporter une technologie en contradiction avec les termes d'un accord d'investissement étranger ou exporter des biens à double usage sans licence ou en contravention avec les textes sont des fraudes douanières caractérisées par plusieurs articles du code des douanes.

– Les sanctions internationales : il entre dans les compétences de la DNRED d'assurer l'application de ces sanctions et de contrer les mécanismes de contournement que peuvent utiliser des personnalités proches de certains régimes ou des entreprises appartenant par exemple à la base industrielle de défense des pays considérés.

– Les flux financiers illicites : l'administration des douanes, en contrôlant les flux financiers physiques – argent liquide, métaux précieux, bijoux… – peut constater des manquements aux obligations déclaratives et des flux qui deviennent du blanchiment au sens douanier du terme s'ils sont le produit d'une activité frauduleuse et criminelle.

– **Les préjudices économiques portés à l'économie française et européenne** par la non-application de la fiscalité européenne sur les importations, et la fraude à la TVA qui lui est généralement adjacente.

– **Le préjudice de nature fiscale**, qui porte atteinte aux intérêts financiers européens ou au budget de l'État, que la TVA associée à ces importations alimente.

b. Le rôle de la CNLRT

La coordination entre services de renseignement en matière de lutte contre les ingérences étrangères incombe à la CNRLT pour ce qui relève du niveau stratégique. *****

La CNRLT se saisit également de sujets ponctuels liés à une menace d'ingérence étrangère qui par leur ampleur et leur caractère systémique préoccupent plusieurs services de la communauté. Elle anime dans ce cadre les réflexions de la communauté et pilote l'élaboration de contre-mesures appropriées. *****

2. Les structures partenaires des services de renseignement

a. Le SGDSN et les agences qui lui sont rattachées : l'ANSSI et VIGINUM

La contre-ingérence mobilise l'appareil d'État, au-delà des seuls services de renseignement à proprement parler. À cet égard, le **Secrétariat général de la défense nationale** (SGDSN) joue un rôle important, en lien avec l'ensemble des services concernés, dans le dispositif de lutte contre les ingérences, et ce dans un grand nombre de champs : cyber, ingérences informationnelles, ingérences dans le domaine académique, de la recherche et de l'innovation, ingérences économiques.

Deux agences sont directement rattachées au SGDSN : l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour ce qui relève de la sécurité des systèmes d'information et de la cyberdéfense et VIGINUM, créé en 2021, qui est le service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères.

i. L'ANSSI

Créée par un décret du 7 juillet 2009, l'ANSSI est un service à compétence nationale rattaché au SGDSN, qui joue le rôle de chef de file dans le dispositif national de cybersécurité, en lien avec les services dédiés au sein des différents ministères, en particulier à l'Intérieur et aux Armées.

L'action de l'ANSSI, partenaire de premier plan des services de renseignement dans le domaine cyber, se décline autour de trois axes :

– La réponse aux cyberattaques.

– La sécurisation des infrastructures informatiques de l'État pour les protéger des attaques extérieures. L'agence est notamment est chargée de proposer ou d'édicter les règles à appliquer pour la protection des systèmes d'information de l'État.

– La diffusion d'une culture de la sécurité numérique dans toute la société par la sensibilisation et la formation au risque cyber.

L'ANSSI et les services de renseignement interagissent dans l'accomplissement de leurs missions respectives. Parmi les quatre chaînes opérationnelles prévues par la Revue stratégique de cyberdéfense de 2018, la chaîne « renseignement » prévoit en effet que « *les services de renseignement contribuent à la politique publique de cyberdéfense pilotée par l'ANSSI et le COMCYBER en assurant la protection de leurs systèmes d'information, en participant à l'anticipation, à la détection et à l'attribution des cyberattaques par la fourniture de renseignement d'intérêt cyber et, dans certains cas, aux actions entreprises dans le domaine de la lutte informatique défensive, de l'action militaire et de l'action judiciaire. Ils réalisent également leurs missions traditionnelles dans le cyberespace, le renseignement d'origine cyber constitue désormais une source importante d'information* ».

ii. VIGINUM

VIGINUM a été créé à l'été 2021 pour protéger le débat public numérique contre les campagnes de manipulation de l'information impliquant des acteurs étrangers et visant à nuire à la France et à ses intérêts fondamentaux.

Dans le contexte d'intensification et d'aggravation des opérations de manipulation de l'information, le SGDSN a piloté fin 2020 en groupe de travail interministériel, appelé « Taskforce Honfleur », chargé de caractériser la dynamique de propagation du discours anti-français circulant sur les plateformes numériques et d'en apprécier le caractère spontané ou non. Il en a conclu qu'une part importante de ces expressions hostiles à la France étaient orchestrées par des acteurs étrangers.

C'est ainsi que le décret du 13 juillet 2021 est venu compléter les dispositions existantes du code de la défense afin de doter le SGDSN de nouvelles attributions en matière de lutte contre les manipulations de l'information, et plus particulièrement contre les ingérences numériques étrangères. Le champ d'intervention de VIGINUM est circonscrit aux thématiques du débat public numérique qui touchent aux intérêts fondamentaux de la Nation, c'est-à-dire au cœur de la souveraineté nationale.

Le fonctionnement de VIGINUM repose sur la notion d'« opération » d'une durée limitée dans le temps telles que la présidence française de l'Union européenne ou l'élection présidentielle. Plusieurs opérations peuvent se dérouler en parallèle. L'agence apporte également son appui au SGDSN dans sa mission d'animation et de coordination des travaux interministériels de lutte contre la menace informationnelle.

VIGINUM est le pivot d'un écosystème national et international plus global œuvrant à la lutte contre les manipulations de l'information.

*****

b. Le SISSE

Le Service de l'information stratégique et de la sécurité économique (SISSE) est né en 2016 de la réunion d'une délégation interministérielle rattachée à Matignon et d'un service de coordination de l'intelligence économique qui dépendait de Bercy. Il est rattaché à la direction générale des entreprises au ministère de l'économie, des finances et de la souveraineté industrielle et numérique.

Le SISSE a pour mission principale le pilotage de la politique de sécurité économique de l'État, qui consiste à organiser la protection des actifs stratégiques de l'économie française face aux ingérences et aux menaces économiques étrangères. Ce service est en quelque sorte la tour de contrôle de ce dispositif de protection. Il organise la coopération entre les nombreux acteurs de cette chaîne d'information et de décision, et rend compte des menaces et des mesures de remédiation prises auprès du Gouvernement.

À l'échelon territorial, le SISSE s'appuie sur un réseau de 22 délégués à l'information stratégique (DISSE) au sein des directions régionales des entreprises (DIRECCTE).

Le SISSE exerce ses fonctions sur la base d'un référentiel constitué de **trois listes couvertes par le secret de la défense nationale** :

– Une liste des entreprises stratégiques pour l'économie française, constituée en 2019. Il s'agit d'une liste *ad hoc* fondée sur des critères de sécurité économique.

– Une liste des technologies critiques pour l'économie française.

– Une liste des laboratoires publics de recherche, économiquement sensibles.

Le SISSE accomplit ses missions dans un cadre interministériel et en lien étroit avec les services de renseignement pour ce qui relève du renseignement de sécurité économique *strico sensu* (et non du renseignement économique en général). Le Service est ainsi destinataire des notes de renseignement économique ***** produites par les services de renseignement. Sur cette base, il va définir ce qui est prioritaire et qui nécessite une intervention de sa part. *****

Le SISSE, par son rôle de détection des phénomènes d'ingérence, est en capacité d'orienter ses capteurs vers tel ou tel mode opératoire et telle ou telle origine géographique et solliciter les services de renseignement pour les surveiller. La fonction du SISSE est à ce jour essentiellement défensive ; or au vu des enjeux croissants de souveraineté liés à la sécurité économique, il serait opportun d'envisager une évolution du périmètre d'action et des moyens humains alloués à ce service. **(Recommandation n° 9)**

3. Une dimension interministérielle renforcée

Compte tenu de la multiplicité des tentatives d'ingérence et de la grande diversité des champs dans lesquels elles se manifestent, l'action de l'État en la matière est par nature interministérielle. L'enjeu de la coordination interministérielle en matière d'influence est rappelé en ces termes par la Revue Nationale Stratégique de 2022 : « *l'influence, dans toutes ses dimensions – diplomatique, militaire, économique, culturelle, sportive, linguistique, informationnelle – est un domaine de contestation, qui nous impose une réponse coordonnée* ». Ainsi, « *la bonne articulation des différentes actions d'influence doit servir une approche intégrée visant à répondre à l'évolution du continuum de menaces que font peser nos adversaires sur nos intérêts et nos valeurs ainsi que ceux de nos plus proches partenaires* ».

Cette dimension interministérielle de la contre-ingérence a été renforcée ces dernières années, tant au niveau stratégique qu'opérationnel dans le cadre de groupes de travail (thématiques et géographiques) réunissant des entités relevant de différents portefeuilles ministériels (Intérieur, Armées, Affaires étrangères, Économie…) sous la coprésidence du SGDSN et de la CNRLT.

Le contexte de la guerre en Ukraine a conforté cette approche. *****

La lutte contre les ingérences étrangères n'est toutefois pas l'affaire des seuls services de renseignement. Ainsi, hors de la communauté du renseignement, la DGSI s'appuie dans sa manœuvre dans le domaine de la contre-ingérence, sur la Direction des libertés publiques et des affaires

juridiques (DLPAJ) du ministère de l'Intérieur au titre des entraves administratives pouvant être conduites. Le ministère de l'Europe et des affaires étrangères constitue également un partenaire majeur dans les différentes thématiques suivies par la sous-direction du contre-espionnage. Une relation spécifique a été nouée avec la direction Europe continentale depuis la guerre en Ukraine, notamment dans le cadre de la politique restrictive sur les visas.

Les priorités que sont la sécurité économique, la cyberdéfense et la lutte contre les ingérences informationnelles illustrent également cette évolution.

En matière de **sécurité économique**, le commissaire à l'information stratégique et de la sécurité économique (CISSE), secondé par le SISSE, exerce, aux côtés du SGDSN, un rôle de coordination interministérielle en matière d'ingérences économiques ; dans ce domaine, la direction générale du Trésor joue également un rôle important en sa qualité de pilote de la procédure de contrôle des investissements étrangers en France.

Depuis 2017, un conseil de sécurité et de défense en format « sécurité économique » se tient régulièrement autour du Président de la République. Le décret du 20 mars 2019 relatif à la gouvernance de la sécurité économique en renforce la collégialité en organisant les travaux des administrations ***** présidé par le SGDSN, et en favorisant le partage de l'information stratégique entre les différents acteurs concernés, pour garantir l'efficacité du dispositif dans son ensemble.

Il consacre le rôle-pivot joué par le SISSE dans l'animation et la mise en œuvre de la politique de sécurité économique. Le commissaire à l'information stratégique et à la sécurité économique ***** et contribue à orienter l'action des services de renseignement vers les priorités identifiées en matière de sécurité économique. Le décret instaure une continuité entre les compétences du commissaire et les missions du SISSE, qui sont regroupées de façon plus lisible autour de trois grands blocs (gestion de l'information stratégique, mise en œuvre des instruments de sécurité économique, promotion des intérêts économiques de la Nation). Parmi les principales nouveautés, le décret confie au SISSE la responsabilité d'organiser la diffusion de l'information stratégique vers les entreprises, et consolide le rôle du SISSE en amont et en aval du régime de contrôle des investissements étrangers en France.

*****

La **cyberdéfense** illustre également cette montée en puissance de la dimension interministérielle dans notre modèle de gouvernance qui,

conformément à **la revue stratégique de cyberdéfense** établie en 2018, distingue un volet offensif et un volet défensif. Dans ce domaine, les services de renseignement interagissent les uns avec les autres et travaillent en lien avec leurs partenaires aux niveaux territorial, national, européen et mondial.

Au niveau stratégique, le Conseil de défense et de sécurité nationale, présidé par le Président de la République, définit les grandes orientations qu'il appartient au Comité de direction (CODIR) cyber (qui réunit le chef d'État-major particulier du Président de la République, le CNRLT et le directeur de cabinet du Premier ministre) de mettre en œuvre. Les membres permanents du CODIR Cyber, dont le secrétariat est assuré par le SGDSN, sont les cabinets du ministère de l'Intérieur et du ministère des Armées, ainsi que les représentants des directions et services directement impliqués dans le domaine de la cyberdéfense.

Au niveau opérationnel, la dimension interministérielle s'incarne à travers **le C4 (Centre de coordination des crises cyber)**, *****

Le **volet influence de la lutte informatique** repose également, autour de VIGINUM, sur une gouvernance interministérielle renforcée. Plusieurs réseaux de coopération ont en effet été mis en place pour assurer un échange fluide et réactif d'informations, une coordination au niveau technique ainsi qu'une approche cohérente face à la menace informationnelle. Au niveau technique, le **réseau Veille, Détection, Caractérisation et Proposition (VDC-P)** rassemble les administrations dotées des capacités techniques en matière de lutte contre les manipulations de l'information. Les échanges sont d'ordre opérationnels, techniques ou méthodologiques.

Au niveau opérationnel, **le Comité opérationnel de lutte contre les manipulations de l'information (COLMI)**, présidé par le SGDSN, réunit la direction des services disposant de capacités opérationnelles ainsi que leurs autorités de rattachement et les représentants des cabinets ministériels concernés. Le comité est notamment chargé de formuler des orientations de travail en matière de lutte contre les manipulations de l'information ainsi que des propositions de réponse face à d'éventuelles ingérences numériques étrangères caractérisées. Au-delà de ces réseaux interministériels techniques et opérationnels, VIGINUM entretient des partenariats avec d'autres administrations. L'agence a ainsi signé en mai 2022 une convention avec le Pôle d'expertise de la régulation numérique (PEReN), service à compétence nationale mettant son expertise en science des données à disposition de l'ensemble des administrations d'État sur les sujets de régulation des plateformes numériques.

C. DES MOYENS DE DETECTION ET D'ENTRAVE MULTIPLES MAIS ENCORE INSUFFISANTS

Pour empêcher les tentatives d'ingérences étrangères, les services de renseignement et, au-delà, la puissance publique, peuvent activer différents dispositifs d'entrave. Bien qu'efficaces, ces outils d'entrave n'en demeurent pas moins parfois insuffisants au regard de l'intensification de la menace que font peser les ingérences étrangères sur l'exercice de la souveraineté nationale et européenne.

1. Une « boîte à outils » pour contrecarrer les ingérences étrangères

La « boîte à outils » des services de renseignement leur permet d'agir de multiples façons pour entraver les tentatives d'ingérences étrangères. Dans le respect du cadre légal et réglementaire, ils peuvent recourir à tout un arsenal juridique pour neutraliser ces actions hostiles qui portent atteinte aux intérêts fondamentaux de la Nation.

a. Le recours aux techniques de renseignement

Les services recueillent du renseignement par le biais de sources humaines ou techniques, capteurs privilégiés dans le cadre d'enquêtes spécifiques sur les auteurs d'actes d'ingérence.

La « *prévention de toute forme d'ingérence étrangère* » correspond à la finalité 2 mentionnée à l'article L.811-3 du Code de la sécurité intérieure (CSI) qui autorise les services de renseignement à recourir aux techniques de renseignement (TR) pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation. En matière de contre-ingérence économique, les services de renseignement exploitent également la finalité 3 mentionnée à l'article L. 811-3 du CSI relative à la *« promotion et prévention des atteintes aux intérêts économiques, industriels et scientifiques majeurs de la France* ».

Les techniques de renseignement autorisées au titre de la finalité 2 sont :

– L'accès aux données de connexion (art. L.851-1 CSI).

– La géolocalisation en temps réel d'un téléphone portable (art. L.851-4 CSI).

– La localisation en temps réel des personnes, véhicules ou objets par le biais d'une balise (art. L.851-5 CSI).

– Le recueil de données par Imsi-Catcher (art. L. 851-6 CSI).

– L'interception de certaines communications hertziennes (art. L.852-2 CSI).

– L'interception des communications satellitaires (art. L.852-3 CSI).

– L'interception de correspondance avec dispositif de type "Imsi-catcher" (art. L. 852-1 CSI).

– La captation, l'enregistrement et la transmission de paroles et d'images
(art. L.853-1 CSI).

– La captation et le recueil de données informatiques (art. L.853-3 CSI).

Le recours aux techniques de renseignement au titre de la finalité 2 est en augmentation significative ces dernières années, surtout depuis 2020. Selon les chiffres communiqués par la CNCTR, le nombre de demandes de TR au titre de cette finalité s'établissait à 17 900 en 2022 contre 13 137 en 2020 et 11 973 en 2017. En proportion de l'ensemble des demandes, la finalité 2 est passée de 16,5 % en 2020 à 20 % en 2022. En revanche, le nombre de personnes surveillées au titre de cette finalité est quasi-stable sur la période, passant de 3 885 à 4 191 entre 2020 et 2022, ce qui signifie que la surveillance est plus intense sur les personnes faisant l'objet d'une technique de renseignement.

LE RECOURS AUX TECHNIQUES DE RENSEIGNEMENT FONDÉ SUR LA FINALITÉ 2

	2018	**2019**	**2020**	**2021**	**2022**
Nombre de demandes de techniques de renseignement	12 460	11 031	13 137	15 327	17 900
En proportion de l'ensemble des demandes	17 %	15 %	16,5 %	17,5 %	20 %
*****	*****	*****	*****	*****	*****

Source : CNCTR.

Au titre de la finalité 2, le recours aux techniques de renseignement peut concerner des personnes dites protégées en raison de la fonction qu'elles exercent (journalistes, avocats, magistrats, parlementaires). Dans ce cas, une procédure assortie de garanties spécifiques est mise en œuvre par la CNCTR qui s'assure en particulier que la demande est proportionnée et détachable de la profession. L'appréciation du caractère détachable de l'exercice d'une profession protégée se révèle parfois complexe en matière de lutte contre les

ingérences étrangères, ladite profession servant parfois de couverture à une action d'ingérence.

*****

b. Les mesures d'ordre diplomatique

Lorsqu'est détecté le comportement suspect d'individus membres d'un service de renseignement étranger, la mesure la plus évidente à prendre est l'expulsion du territoire national, dans le cadre de mesures dites de ***persona non gratae*** **(PNG).** Ces mesures avaient notamment été utilisées dans les années 1980 à l'égard des services russes.

Les dernières vagues de PNG furent consécutives à l'invasion de l'Ukraine par la Russie. 41 déclarations PNG ont été prononcées en deux temps : au printemps 2022, à la suite de la révélation du massacre de Boutcha, la France, comme l'Allemagne et d'autres pays européens, a procédé à l'expulsion de 35 officiers de renseignement russes sous couverture diplomatique ; une semaine plus tard, six autres officiers de renseignement russes sous couverture diplomatique ont également été visés par une mesure de PNG après la mise à jour en flagrant délit, par la DGSI, du traitement d'une source sur le territoire national. À cela, s'ajoutent près de 500 fiches d'interdiction d'accès au territoire émises au fichier des personnes recherchées (FPR) à l'encontre d'officiers de renseignement russes. 23 opérations disruptives ont également été conduites en 2022 afin de faire cesser une relation ou des actions malveillantes (sensibilisation individuelle de personnes approchées, mise en garde d'agent de renseignement, etc.).

La fermeture de la représentation russe au Conseil de l'Europe à l'été 2022 a également permis le départ d'un nombre significatif d'officiers de renseignement russes agissant sous couverture diplomatique.

Par ailleurs il a également été procédé ces dernières années à plusieurs demandes de rappel silencieux : s'il n'est pas toujours estimé opportun, du point de vue diplomatique, d'expulser un diplomate, il est alors demandé au pays dont le comportement de l'agent s'inscrit en violation de la Convention de Vienne, de procéder silencieusement à son rappel.

***** **(Recommandation n° 10)**

c. Les mesures pénales

Le dispositif légal français pour lutter contre l'espionnage prévoit des infractions spécifiques d'atteintes aux intérêts fondamentaux de la Nation (IFN).

L'article 410-1 du code pénal définit les IFN comme « *son indépendance, l'intégrité de son territoire, sa sécurité, la forme républicaine des institutions, les moyens de sa défense et de sa diplomatie, la sauvegarde de sa population en France et à l'étranger, l'équilibre de son milieu naturel et de son environnement et les éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel* ».

Les IFN couvrent ainsi non seulement toute information relative à la situation militaire ou diplomatique de la France mais également, au-delà des seules dimensions régaliennes de son action, ses intérêts économiques essentiels. Plusieurs infractions sont prévues :

– La livraison de toute ou partie du territoire national, des forces armées ou de matériel à une puissance étrangère.

– Les intelligences avec une puissance étrangère.

– La livraison d'informations à une puissance étrangère.

– Le sabotage.

– La fourniture de fausses informations.

– La provocation à la trahison ou l'espionnage.

– Les atteintes au secret de la défense nationale.

Parmi les procédures judiciaires ouvertes sur le fondement du livre IV du code pénal, on peut citer l'arrestation, à l'été 2020, d'un militaire de haut rang de l'armée française, en poste à l'OTAN à Naples, poursuivi pour des faits d'espionnage et de trahison. On peut également citer la condamnation de deux anciens agents d'un service de renseignement français, détectés grâce au travail attentif de leur service d'affectation, judiciarisés par la DGSI et déclarés coupables d'espionnage au bénéfice des services chinois.

En matière pénale, une des principales problématiques concerne toutefois l'opportunité d'engager des poursuites. En effet, l'intérêt à faire condamner un individu peut être contrebalancé par le risque d'un échec des poursuites et de la révélation des sources humaines, techniques de renseignement et modes opératoires engagés par un service de renseignement.

d. Les mesures d'ordre économique

Il existe différents outils d'entrave en matière de sécurité économique, parmi lesquels figurent le **dispositif de contrôle des investissements étrangers dans les entreprises sensibles** ainsi que la **loi de blocage** visant à

empêcher la transmission à des autorités publiques étrangères de « *documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique qui serait de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public* ».

Les investissements étrangers en France (IEF) sont dans leur majorité une opportunité et la France se doit de rester attractive pour les capitaux étrangers ; mais sans naïveté. Aussi, un dispositif de contrôle des IEF prévoit que ceux qui présentent des enjeux en termes d'ordre et de sécurité publics, ou de défense nationale sont soumis à l'autorisation préalable du ministre de l'Économie et des Finances, par exception au principe général de libre circulation des capitaux. Afin d'adapter le dispositif français aux défis contemporains que peuvent représenter certains investissements étrangers, **la liste des secteurs concernés par le contrôle des investissements étrangers a été modifiée par le décret n° 2018-1057 du 1er décembre 2018** relatif aux investissements étrangers soumis à autorisation préalable. Depuis le 1er janvier 2019, les entreprises dans les secteurs de l'aérospatial et de la protection civile, ou qui mènent des activités de recherche et de développement en matière de cybersécurité, d'intelligence artificielle, de robotique, de fabrication additive, de semi-conducteurs, ainsi que les hébergeurs de certaines données sensibles, entrent dans le champ du contrôle. Cela signifie qu'une opération d'investissement au sens de la règlementation portant sur le contrôle des investissements étrangers s'applique dès lors qu'elle permet le franchissement du seuil de 25 % des droits de vote au sein du conseil d'administration. **Depuis juin 2020, dans le contexte de la crise sanitaire, ce seuil a été abaissé à 10 %,** initialement jusqu'au 31 décembre 2022, avec une prorogation jusqu'au 31 décembre 2023. Depuis 2021, on constate une très forte croissance des dossiers IEF, dépassant les 300 cas par an.

La loi de blocage du 26 juillet 1968 a été adoptée pour protéger les informations et données sensibles attentant aux intérêts de la Nation, qui pourraient être communiquées comme preuves à l'occasion de procédures judiciaires à l'étranger. Cette loi vient notamment en réponse à l'utilisation par les juridictions américaines de la procédure *Discovery*, permettant de communiquer des données stratégiques lors de procès avec des entreprises concurrentes.

Ce dispositif *Discovery* est une procédure de collecte de preuves dans le cadre de la phase d'instruction préalable au procès. Il s'agit d'une mesure à caractère extraterritorial puisqu'elle s'impose à toute personne, physique ou morale, impliquée dans la procédure, nationale ou étrangère, et concerne tout élément de preuve, quelle que soit leur forme ou leur localisation. La procédure de *Discovery* est très régulièrement utilisée par les juridictions

américaines dans le cadre de procès civils et peut être étendue à des domaines qui dépassent l'objet même du contentieux.

La loi de blocage de 1968 interdit ainsi la demande, la recherche ou la communication, directe ou indirecte, de documents d'ordre économique, commercial, industriel, financier ou technique dans le cadre de procédures judiciaires ou administratives étrangères, sous réserve des traités internationaux en vigueur. Elle s'applique à toute preuve située en France, qu'elle soit détenue par une personne physique ou morale, nationale ou étrangère.

Bien que la loi soit qualifiée de « blocage », elle n'a pas pour objectif d'empêcher la transmission de données à des autorités judiciaires étrangères en cas de litige mais de restreindre l'utilisation du dispositif *Discovery* et d'obliger les autorités étrangères à respecter les canaux de la coopération judiciaire et administrative internationale.

Face à l'utilisation croissante de lois à portée extraterritoriale par des acteurs étrangers et au caractère peu dissuasif de la loi de blocage, le décret du 18 février 2022 et l'arrêté du 7 mars 2022 ont clarifié la procédure pour les entreprises, et désigné comme interlocuteur unique le Service de l'information stratégique et de la sécurité économiques (SISSE).

Le SISSE accompagne ainsi les entreprises françaises, en lien avec les différentes administrations de l'État, pour faire face aux demandes des juridictions étrangères. Il s'agit également de renforcer la sécurité juridique des entreprises en leur permettant de disposer d'un avis de l'administration française afin de renforcer le caractère opposable de la loi de blocage vis-à-vis des juridictions étrangères.

e. Le dispositif de protection du potentiel scientifique et technique de la nation (PPST)

Le dispositif de **protection du potentiel scientifique et technique de la nation (PPST)** vise à protéger les savoirs, expertises et technologies les plus « sensibles » des établissements publics et privés (laboratoires de recherches, entreprises, etc.) localisés sur le territoire national, dont le détournement ou la captation pourrait porter atteinte aux intérêts économiques de la Nation, renforcer des arsenaux militaires étrangers ou affaiblir les capacités de défense françaises, contribuer à la prolifération des armes de destruction massive et de leurs vecteurs ou être utilisées à des fins terroristes.

Le dispositif PPST est dirigé au sein de chaque ministère par un Haut fonctionnaire de défense et de sécurité qui anime un réseau de fonctionnaires

de sécurité et de défense (FSD) au niveau des établissements d'enseignement supérieur.

Fondé sur l'article 413-7 du code pénal, ce dispositif interministériel piloté par le SGDSN est déployé par les ministères chargés de l'agriculture, de la défense, de l'économie, de l'énergie, de l'environnement, de la recherche, de la santé et des transports qui y concourent par l'intermédiaire de six hauts fonctionnaires de défense et de sécurité, chacun adaptant les modalités de mise en œuvre en fonction des spécificités de son champ de compétence.

Le dispositif de PPPST rend possible la création de « zones à régime restrictif » (ZRR), qui permettent de soumettre à un contrôle les accès physiques aux lieux concernés par des informations sensibles en cas de vol ou de pillage de leurs savoir-faire et de les protéger juridiquement, ce faisant, d'actes malveillants.

Deux décrets, publiés en mars 2022 sont venus optimiser le traitement des demandes d'accès en ZRR afin de réduire les délais d'instruction des avis relatifs aux demandes d'accès. Entre 2021 et 2022, le nombre de ZRR a augmenté de 11 %.

Le dispositif de PPST mériterait d'être renforcé. En effet, comme le souligne le rapport Gattolin, le seuil de vigilance est trop haut et ne s'applique qu'à des risques très élevés de savoirs et savoir-faire. Par ailleurs, il n'est pas adapté aux nouvelles stratégies d'influences qui ciblent, au-delà des sciences dites dures, les sciences humaines et sociales. Enfin, son champ est limité au patrimoine matériel ce qui rend le dispositif de protection inopérant pour le patrimoine numérique. C'est pourquoi il serait pertinent **d'étendre le dispositif de PPST au patrimoine immatériel ainsi qu'à l'ensemble des disciplines universitaires** notamment en l'adaptant aux enjeux et influences spécifiques aux sciences humaines et sociales qui en sont exclues. **(Recommandation n° 11)**

En outre, le régime juridique des ZRR, aussi efficace soit-il, est limité à l'accès physique aux informations sensibles, et ne couvre pas l'accès dématérialisé, ce qui limite sa portée.

Enfin, force est de constater un manque global de moyens, de coordination et de sensibilisation de la communauté académique à l'émergence de ces nouvelles menaces. Faute de moyens dédiés, les fonctions de FSD, quand elles existent, sont généralement occupées par un vice-président de l'Université ou le directeur général de l'établissement. Afin de conforter les fonctions de sûreté et de défense au sein des universités, la Délégation recommande d'inscrire ce poste dans le référentiel interministériel des métiers de l'État. **(Recommandation n° 12)**

f. Les dispositions issues de la loi « séparatisme » du 24 août 2021 confortant le respect des principes de la République

L'entrée en vigueur de la loi du 24 août 2021 confortant les principes de la République (CRPR), et de ses décrets d'application, a donné aux services de l'Etat de nouveaux leviers d'entrave sur les associations exerçant le culte et étant contrôlée, partiellement ou totalement par des puissances étrangères.

La loi renforce **le contrôle des associations cultuelles et des lieux de culte**. Les conditions de création et de gouvernance des associations gérant un lieu de culte prévues par la loi de 1905 ont été revues afin de les protéger des prises de contrôle malveillantes par des groupes radicaux (clause dite anti-putsch). Ces associations cultuelles doivent désormais se déclarer auprès du préfet tous les cinq ans et voient leurs obligations comptables renforcées.

À cet égard, ont permis d'améliorer les capacités d'entrave à l'encontre des financements occultes des associations cultuelles par des puissances étrangères :

– Tout d'abord, l'élargissement de la définition des associations exerçant le culte : sont désormais considérées comme « exerçant le culte » non seulement celles déclarées sons la forme juridique dite « loi 1905 », mais également toute association mentionnant dans ses statuts l'exercice d'activités cultuelles (c'est-à-dire : tenue d'une cérémonie de culte, formation d'imams, salaires des imams, entretien d'un édifice cultuel, etc.), ce qui est le cas de nombreuses associations enregistrées sous le statut de la loi de 1901, qui se voient désormais appliquées les mêmes obligations que les associations sous le statut de la loi de 1905.

– Ensuite, l'obligation prévue à l'article 77 de la loi (nouvel article 19-3 de la loi de 1905) faite aux associations exerçant le culte de déclarer tous les financements étrangers (directs ou indirects) au-delà du seuil de 15 300 euros annuels. L'autorité administrative peut s'opposer au bénéfice des avantages et ressources obtenues d'une puissance étrangère lorsque les agissements de l'association bénéficiaire ou de l'un de ses dirigeants établissent l'existence d'une menace réelle, actuelle et suffisamment grave affectant un intérêt fondamental de la société. Des sanctions pénales sont également prévues en cas de non-respect de cette obligation.

– Enfin, le respect d'un certain nombre d'obligations de transparence financière (publication des comptes et transmission au préfet à sa demande).

Dans le cadre du dispositif mis en œuvre pour lutter contre le séparatisme, la DGSI, qui est chargée de suivre les principaux acteurs

d'influence des pays du Maghreb, de Turquie et des pays du Golfe s'agissant des questions relatives à l'exercice du culte musulman en France, participe au comité de suivi des financements étrangers, piloté par la CNRLT. Son rôle consiste à suivre les déclarations des financements étrangers aux niveaux zonal et central, mais également de signaler les financements non déclarés dont elle aurait connaissance par le biais de ses capteurs techniques et humains *****. La DGSI intervient en lien avec **Tracfin qui mobilise ses leviers d'action pour détecter le financement étranger des lieux de culte**. Le service de renseignement financier a ainsi pris un certain nombre de mesures d'entrave de l'activité marocaine et algérienne en lien avec la Grande Mosquée de Paris. Depuis l'entrée en vigueur de la loi, il ressort que les financements de lieux de culte sur le territoire national émanant de pays du Maghreb, de Turquie et du Moyen-Orient sont en très net recul.

Une autre disposition de la loi CRPR concerne **le financement des écoles privées hors contrat** qui doivent désormais répondre à de nouvelles obligations. Un régime de fermeture administrative des écoles non déclarées ou qui n'ont pas remédié aux défaillances constatées par l'administration est créé. Les préfets peuvent désormais s'opposer à l'ouverture d'écoles hors contrat soutenues par un État étranger hostile à la République.

La loi CRPR a incontestablement emporté des effets positifs par l'apport de nouveaux outils mais aussi par son rôle dissuasif vis-à-vis de certains acteurs qui se sont en effet régularisés de leur propre initiative.

Néanmoins, cette loi connait certaines limites :

– Elle ne prend pas en compte les terrains non bâtis. Or, de nombreuses associations poursuivent des projets d'acquisition de terrains afin d'y construire des centres culturels ou des mosquées. Si la loi CRPR prévoit une obligation d'autorisation préalable du préfet lorsqu'il s'agit de bâtiments servant habituellement à l'exercice public du culte, ce n'est pas le cas pour les terrains non bâtis.

– Elle n'aborde pas la transparence financière des dons et l'appel à la générosité du public ;

– Elle ne prévoit pas de dispositif spécifique pour contrecarrer le recours excessif aux sociétés civiles immobilières pour financer et soutenir les associations exerçant le culte. Or, si la loi de 1905 précise que ces associations peuvent détenir des biens immobiliers lorsque cette détention est en lien avec leur objectif social, il apparaît que nombre d'associations cultuelles ne peuvent justifier d'un tel lien.

Aussi, la bonne application des nouveaux outils issus de cette loi ne représente qu'une partie de l'action des services de renseignement, en particulier de la DGSI, sur le volet financier des vecteurs d'influence étrangers dans le culte musulman. *****

2. Des nouveaux moyens d'entrave sont nécessaires pour contrecarrer des actions hostiles à nos intérêts fondamentaux

La notion d'ingérences étrangères dépasse désormais celle de l'espionnage « classique » pour laquelle les services disposent d'outils législatifs adaptés, à travers les qualifications relevant du titre I^er^ du livre IV du code pénal, relatif aux crimes et délits d'atteinte aux intérêts fondamentaux de la nation, comportements d'espionnage et de trahison au sens strict et atteintes au secret de la défense nationale (compromission).

Les services de renseignement sont en effet confrontés à des tentatives d'ingérences politiques étrangères visant à tisser des relations personnelles avec des agents publics et des acteurs politiques pour faire avancer des intérêts étrangers qui n'entrent pas dans le cadre juridique existant. Aussi, de nouveaux dispositifs paraissent nécessaires pour renforcer notre arsenal juridique face aux ingérences étrangères, potentielles ou réelles.

a. Permettre au ministre des Armées de s'opposer au recrutement par un État ou une entreprise étrangère de militaires nationaux détenteurs de savoir-faire militaires opérationnels rares

Jusqu'à l'entrée en vigueur de la loi de programmation militaire 2024-2030, aucun dispositif juridique ne permettait d'empêcher *a priori* le départ de militaires recrutés par un État ou une entreprise étrangère. Or les tentatives de recrutement de militaires français par des puissances étrangères se multiplient. On estime à une dizaine le nombre de pilotes français de *Rafale* ayant été approchés ces dernières années en raison de leur maîtrise de savoir-faire opérationnels rares comme le décollage par catapulte ou encore l'appontage.

Le code pénal (art. 411-6 à 411-8) punit le fait d'entretenir des intelligences avec une entité étrangère et le fait de recueillir ou de rassembler des informations ou supports en vue de la livraison à une entité étrangère. Mais pour caractériser l'infraction d'intelligence avec une entité étrangère, il importe de recueillir des éléments matériels prouvant que l'auteur a agi volontairement et ayant pleinement conscience de porter atteinte aux intérêts fondamentaux de la Nation dont il est ressortissant.

Or la collecte et conservation de données au profit d'une entité étrangère punies ne correspondent pas par exemple à la livraison d'un

savoir-faire militaire opérationnel comme la technique d'appontage pour un pilote de *Rafale*. Ainsi, l'ensemble de ces dispositifs ne permettent pas de prévenir le départ d'un militaire vers une puissance étrangère en vue de lui livrer un savoir-faire militaire opérationnel.

Aussi, la loi de programmation militaire pour les années 2024 à 2030 permet désormais, à l'instar de ce qui existe notamment aux États-Unis, la mise en œuvre **d'un régime préventif de contrôle des départs des militaires recrutés par des puissances étrangères.** Il instaure, pour les militaires exerçant des fonctions présentant une sensibilité particulière ou requérant des compétences techniques spécialisées, un régime de déclaration préalable obligatoire au Ministre des Armées lorsqu'ils souhaitent « *exercer une activité en échange d'un avantage personnel ou d'une rémunération dans le domaine de la défense ou de la sécurité au bénéfice d'un État étranger ou d'une entreprise ou d'une organisation ayant son siège en dehors du territoire national ou sous contrôle étranger* ». Ce régime de déclaration préalable obligatoire s'applique dans les dix ans suivant la cessation des fonctions, cette durée correspondant à la durée moyenne au terme de laquelle le savoir-faire des intéressés est présumé devenu obsolète.

Les militaires concernés sont ceux qui occupent des emplois sensibles relevant par exemple du commandement dans le domaine naval, de la cyberdéfense, du secteur du nucléaire ou encore du renseignement. Le ministre des Armées pourra désormais s'opposer au recrutement par une entité étrangère d'un ancien militaire français dans deux cas :

– S'il estime que cet exercice comporte le risque d'une divulgation par l'intéressé de renseignements, procédés, objets, documents, données informatisées ou fichiers auxquels il a eu accès dans le cadre de ces fonctions.

– Si cette divulgation est de nature à porter atteinte aux intérêts fondamentaux de la Nation

Le périmètre du dispositif est large puisqu'il inclue « l*e bénéfice direct ou indirect à un État ou une entreprise étrangère, les collectivités territoriales étrangères* ». Il concerne également les agents civils de l'État ou de ses établissements publics participant au développement de savoir-faire nécessaires à la préparation et à la conduite des opérations militaires. En revanche, ne sont pas concernés les militaires qui souhaiteraient exercer une activité au sein d'une entreprise titulaire d'une autorisation d'exportation de matériel de guerre français.

b. Instaurer un dispositif législatif spécifique aux ingérences étrangères, à l'instar de ce qui existe dans certains pays

Plusieurs pays ont adopté ou débattent actuellement de législations visant à assurer une meilleure visibilité à la prévention des ingérences étrangères, qui reposent sur la création d'un registre des agents étrangers conduisant des actions d'ingérence dans la vie publique. C'est notamment le cas des États-Unis, de l'Australie, du Canada et du Royaume-Uni. La Commission européenne a également annoncé la présentation prochaine, vraisemblablement à l'automne 2023, d'un « paquet législatif » sur la « Défense de la démocratie ».

Si la France dispose, depuis la loi Sapin 2, d'un dispositif de transparence des représentants d'intérêt, ce régime apparaît insuffisant dès lors qu'il a été conçu pour viser principalement les activités de lobbying économique et se révèle insuffisamment adapté aux spécificités de l'action d'influence étrangère. Par ailleurs, la circulaire du Premier ministre du 11 octobre 2021, relative au renforcement de la transparence des actions d'influence étrangère conduites auprès des agents publics de l'Etat, ne couvre pas non plus l'intégralité des actions d'ingérence menées dans la vie publique.

C'est pourquoi l'adoption d'un dispositif de transparence *ad hoc*, spécifique aux ingérences étrangères, aurait le mérite :

– De distinguer clairement la problématique du lobbying économique et celle de l'influence étrangère.

– D'espérer attraire dans le champ du nouveau registre un nombre plus important d'agents d'influence que ceux qui relèvent du champ du registre actuel de la loi Sapin 2.

– D'envoyer un signal politique fort dans un contexte géopolitique marqué par la résurgence des ingérences étrangères.

Un tel dispositif *ad hoc* aurait pour objet de **rendre obligatoire l'enregistrement des acteurs influant sur la vie publique française pour le compte d'une puissance étrangère et de les soumettre à une série d'obligations déontologiques**. La finalité d'un tel enregistrement serait double : d'une part, limiter les tentatives d'influence, voire d'ingérence étrangère sur l'action publique française et d'autre part, renforcer l'information des responsables publics et des élus sur la nature de leurs interlocuteurs étrangers.

L'obligation de déclaration s'imposerait à toute personne physique ou morale qui, de manière cumulative :

– Conduirait une activité d'influence sur la décision publique, notamment sur le contenu d'une loi ou d'un acte réglementaire, sur la conduite des politiques publiques ou sur un processus électoral.

– Conduirait cette activité pour le compte, sous la direction ou le contrôle d'une puissance étrangère, aux fins de promouvoir les intérêts de cette puissance étrangère.

À l'instar du régime des représentants d'intérêt, la gestion de ce régime déclaratif pourrait être confiée à la Haute autorité de contrôle de la vie publique (HATVP). **Un régime de sanctions pénales serait instauré en cas de non-respect de l'obligation de déclaration.**

Alors que la Commission européenne travaille à la présentation d'un train de mesures européennes visant à lutter contre les ingérences étrangères, la mise en place en France d'un dispositif *ad hoc* pourrait aussi préfigurer la création d'un « FARA » européen. **(Recommandation n° 13)**

LE NATIONAL SECURITY BILL :

Une adaptation majeure du cadre juridique anglais pour lutter contre les ingérences étrangères

En mai 2022, le Parlement britannique a été saisi d'un projet de loi qui vise à moderniser substantiellement la loi de contre-espionnage datant de 1911 pour l'orienter vers une stratégie de contre-ingérence. Le *National Security Bill*, est entré en vigueur le 11 juillet 2023.

Ce projet de loi comprend trois principaux volets :

1. Le renforcement du champ infractionnel et des pouvoirs d'investigation en matière de contre-espionnage et de contre-ingérence avec la création de nouvelles infractions en matière de contre-espionnage, comme par exemple le fait de conduire des activités de sabotage pour le compte d'une puissance étrangère. Le National Security Bill crée également de nouvelles infractions spécifiques à la lutte contre les ingérences étrangères : une infraction générale réprimant les actions d'ingérence dès lors que certaines conditions sont réunies, une infraction spécifique à l'ingérence dans les élections politiques du Royaume-Uni (en réprimant notamment l'utilisation de fausses identités dans une campagne électorale pour promouvoir les intérêts d'une puissance étrangère). Le texte crée également une infraction préparatoire réprimant les personnes engagées dans la conduite préparatoire à la commission d'une infraction en lien avec une ingérence étrangère.
2. La mise en place de mesures administratives restrictives à l'encontre d'individus soupçonnés de conduire des actions d'ingérence, telles que l'assignation à résidence, des restrictions d'accès à certains lieux, l'interdiction de quitter le Royaume-Uni, l'obligation de se présenter à un poste de police, etc.
3. La création d'un registre des agents de l'étranger (*Foreign Influence Registration Scheme* – FIRS), qui s'inspire des dispositifs américains (FARA, adopté en 1938) et australien (*Foreign influence transparency scheme* – FITS, adopté en 2018). Il s'agit d'un dispositif visant à rendre obligatoire l'enregistrement dans un registre dédié de personnes agissant pour le compte d'une puissance étrangère à des fins d'influence de la vie publique.

c. Expérimenter l'extension aux finalités 1 et 2 de la technique de l'algorithme

La technique de renseignement dite de l'algorithme, introduite à titre expérimental dans notre droit depuis la loi du 24 juillet 2015 et pérennisée par la loi du 30 juillet 2021 permet un traitement automatisé des données de connexion et de navigation sur Internet, grâce à la coopération des fournisseurs d'accès, aux fins de détecter des comportements associés à une menace.

Le recours à cette technique est toutefois exclusivement limité à la finalité 4 liée à la prévention du terrorisme. Or en matière de contre-espionnage et de contre-ingérence, la technique de l'algorithme serait de nature à renforcer les capacités de détection précoce de toute forme d'ingérence ou de tentative d'ingérence étrangère des services de renseignement.

Il est en effet possible de modéliser les méthodes opératoires propres à certains services de renseignement étrangers agissant sur le territoire national, en termes de déplacements comme d'habitudes de communication, de manière à détecter sur les réseaux des opérateurs téléphoniques des comportements susceptibles de révéler une menace pour les intérêts fondamentaux de la Nation.

*****

Aussi la Délégation propose, **à titre expérimental et pour une durée de 3 ans, d'élargir le champ d'application de la technique de l'algorithme aux finalités 1** (« indépendance nationale, intégrité du territoire et défense nationale ») **et 2 (**« intérêts majeurs de la politique étrangère, exécution des engagements européens et internationaux de la France et prévention de toute forme d'ingérence étrangère »). Au terme de cette expérimentation, il est proposé qu'un rapport d'évaluation soit remis à la Délégation parlementaire au renseignement. **(Recommandation°14)**

d. Élargir aux ingérences étrangères le périmètre de la procédure des gels d'avoirs

Le Code monétaire et financier permet de geler pour une durée de six mois renouvelables les fonds et ressources économiques de toute personne morale ou physique impliquée dans des actions au profit de groupes terroristes. Ces mesures nationales de police administrative sont toutefois limitées au périmètre des individus et structures liées à des groupes inscrits sur la liste des organisations terroristes. Elles sont complétées par des régimes internationaux (ONU et UE) ; de même il existe des régimes spécifiques de gel des avoirs pour lutter contre la prolifération d'armes de destruction massive ou les cyberattaques, ainsi que des régimes géographiques (pays sous sanctions).

La Délégation considère opportun d'élargir le spectre des gels d'avoirs à but antiterroriste (GABAT) à toute personne ou structure se livrant à des actions préjudiciables au maintien de la cohésion nationale ou destinée à favoriser les intérêts d'une puissance étrangère. Une extension du régime GABAT pourrait utilement viser les manœuvres de contournement de la règlementation, en lien avec une puissance étrangère. Le régime devrait

conserver sa vocation préventive : le gel serait prononcé sur une personne morale ou physique qui agirait de manière avérée afin de contourner la réglementation. La personne visée aurait alors six mois pour se mettre en conformité avec la réglementation et / ou prouver sa bonne foi aux autorités. **(Recommandation°15)**

e. Apporter une réponse européenne aux tentatives de déstabilisation liées aux ingérences étrangères

Par une décision du 18 juin 2020, le Parlement européen a créé une commission spéciale, initialement pour une durée d'un an mais prolongée de six mois, sur « *l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation* » (INGE 1)

Dans son rapport adopté en séance plénière à Strasbourg le 9 mars 2022, le Parlement européen conclut que « *des acteurs malveillants ont bel et bien influencé les élections, mené des cyberattaques, embauché d'anciens hauts responsables politiques et accru la polarisation du débat public, sans crainte de répercussions* ». Les députés européens ont mis en avant le manque de définition et de compréhension communes de ce phénomène des ingérences étrangères et les nombreuses lacunes et failles qui demeurent dans la législation et les politiques actuelles tant au niveau de l'Union qu'au niveau national pour détecter et prévenir les ingérences étrangères et lutter contre celles-ci.

Dès le lendemain de l'adoption du rapport, le Parlement européen a décidé de la constitution d'une nouvelle commission spéciale, INGE 2, dont le mandat prévoit qu'elle est notamment chargée de recenser les lacunes, les failles et les chevauchements des législations en vigueur, de déterminer la base juridique appropriée pour tout acte juridique nécessaire et de préparer le terrain à des solutions institutionnelles permanentes de l'Union pour lutter contre l'ingérence malveillante étrangère et la désinformation et, si nécessaire, de demander à la Commission de prendre des mesures institutionnelles spécifiques.

Une prise de conscience est clairement en train de s'opérer à l'échelle européenne et **le scandale du *Qatargate*, inédit par son ampleur, a provoqué un électrochoc et appelle à une réponse globale et coordonnée avec les États membres.**

Dans la guerre commerciale qui oppose l'Europe à la Chine, l'Union européenne est ainsi parvenue le 28 mars 2023 à adopter **un instrument anti-coercitif contre l'ingérence étrangère**. Ce nouveau règlement va permettre à l'Union de prendre des contre-mesures, telles que des droits de douane, des restrictions commerciales ou des mesures relatives aux marchés publics, à l'encontre des pays tiers qui tentent de faire pression sur les États membres ou

les institutions européennes. Si la Commission européenne et une majorité qualifiée d'États membres s'accordent à dire qu'un pays tiers a eu recours à la coercition, ils pourraient d'un commun accord, en lien avec le Parlement européen, décider d'un ensemble de contre-mesures à prendre à l'encontre du pays en question. Avec ce nouvel instrument juridique, la Chine mais aussi les États-Unis qui menacent régulièrement l'Union européenne de tarifs douaniers punitifs si elle mettait en œuvre une taxe numérique défavorable aux grandes entreprises américaines, sont dans le viseur des Européens.

La Commission européenne a également annoncé, dans le cadre d'un futur train de mesures « **Défense de la démocratie** », sa volonté d'élaborer des mesures législatives (normes communes de transparence et de responsabilité pour les services de représentation d'intérêts dirigés ou payés depuis des pays tiers) et non législatives (recommandations sur l'ingérence secrète de pays non-membres de l'Union, adressées aux États membres aux partis politiques nationaux et européens et éventuellement à d'autres entités) pour « *renforcer la résilience face à l'ingérence étrangère déguisée dans notre vie démocratique* ». Cette démarche, qui intervient en amont des élections européennes du printemps 2024, pourrait s'inspirer des dispositifs adoptés ou en cours d'adoption à l'étranger.

Au vu des conclusions du rapport de la Commission spéciale INGE 1 et de cette volonté politique de la Commission européenne, la Délégation considère qu'une réponse européenne appropriée face aux ingérences étrangères pourrait s'orienter dans trois directions :

– La mise en place d'instruments juridiques contraignants assortis d'un régime de sanctions, à l'instar de ce qui existe dans différents pays (notamment les États-Unis, l'Australie et prochainement le Royaume-Uni) afin de mettre un terme à une forme d'impunité d'actions de déstabilisation et de campagnes de désinformation conduites par des entités étrangères. Il conviendrait en particulier de donner une force contraignante au code de bonnes pratiques de l'Union européenne contre la désinformation en ligne, dont *Twitter* a décidé de s'affranchir sans autres conséquences.

– L'amélioration du dispositif européen de cybersécurité, avec des moyens humains et financiers adaptés aux défis et la garantie que la sécurité des infrastructures stratégiques ne dépende pas de technologies étrangères. L'Union européenne pourrait également promouvoir l'élaboration d'un traité international relatif à la cybersécurité qui fixerait des normes internationales en matière de cybersécurité pour lutter contre la cybercriminalité.

– La définition d'un **partenariat stratégique entre les différents acteurs et structures de l'Union européenne et des États membres** pour assurer une coordination efficace ***** **(Recommandation°16)**

***

Le contexte national, européen et international rend assurément le moment opportun pour renforcer l'arsenal juridique visant à mieux nous protéger des ingérences étrangères. Les esprits évoluent et la conflictualité permanente des relations internationales favorise une prise de conscience tardive mais réelle de l'opinion publique. Le renseignement participe d'une réponse globale à la menace omniprésente des ingérences étrangères. **Nous avons plus que jamais besoin d'un débat public sur la réponse démocratique aux ingérences étrangère**s. Les recommandations de la Délégation parlementaire au renseignement visant à nous doter de nouveaux moyens d'entrave pourraient à cet égard être rassemblées dans **un projet de loi dédié à la lutte contre les ingérences étrangères** et qui soulignerait la contribution du renseignement à notre riposte démocratique **(Recommandation n° 17)**.

III. LES POSITIONS STRATÉGIQUES FRANÇAISES À L'ÉPREUVE DES INGÉRENCES ÉTRANGÈRES EN AFRIQUE AUSTRALE ET DANS L'OCÉAN INDIEN

Le Président de la Délégation parlementaire au renseignement a effectué, du 16 au 22 avril 2023, un déplacement en Afrique du Sud, à l'Île de la Réunion puis à Madagascar au cours duquel des entretiens ont été réalisés avec les représentations diplomatiques et préfectorales, les différents services de renseignement présents dans les territoires visités ainsi que les attachés de sécurité intérieure (ASI) et de défense.

Le choix des pays et du département français d'outre-mer visités a fait suite à des échanges préalables avec les directeurs généraux de la sécurité intérieure et de la sécurité extérieure au vu des enjeux liés à la thématique des ingérences étrangères. Si un déplacement au Sahel eût été justifié au vu du retrait des forces françaises et de la place prise par la milice privée Wagner, il a semblé plus pertinent de se rendre dans une zone certes à ce jour moins exposée militairement et médiatiquement mais néanmoins sujette à de véritables guerres d'influence entre puissances étrangères et qui préparent le terrain aux ingérences de demain.

En Afrique Australe et dans l'océan indien, la France a des intérêts majeurs à défendre et notre appareil de renseignement joue un rôle essentiel pour révéler les stratégies, mesurer les enjeux et préparer l'avenir.

*****

A. RENSEIGNER POUR DÉTECTER ET SURVEILLER LES PHÉNOMÈNES D'INGÉRENCES

1. Les raisons d'être d'un climat d'ingérences

Au moins trois facteurs principaux expliquent le climat d'ingérences qui règne dans cette partie du monde : le terreau favorable que constituent des États faillis ou *a minima* très affaiblis, des liens historiques avec des puissances étrangères et enfin, un contexte géopolitique très singulier.

a. Des États faillis

Les cas sont de plus en plus nombreux sur le continent Africain d'États dont l'affaiblissement est tel qu'ils deviennent le terreau d'ingérences étrangères plus ou moins assumées. La zone sahélienne est emblématique de ce phénomène comme au Mali où l'effondrement de l'État a laissé le champ

libre aux mercenaires de Wagner dans le contexte du redéploiement de l'opération militaire française Barkhane.

Le groupe paramilitaire russe est d'ores et déjà bien implanté dans plusieurs pays sur le continent et a le regard tourné vers d'autres États comme le Burkina-Faso mais aussi le Cameroun *****. La situation en République Centrafricaine (RCA) est quant à elle symptomatique d'un processus d'ingérence qui prend sa source dans l'autorisation accordée à la Russie de vendre des armes aux forces armées centrafricaines, en dérogeant à l'embargo qui pesait sur la Centrafrique, en guerre civile depuis 2013. Le réarmement des forces armées centrafricaines (FACa), nécessitant la levée de l'embargo sur les armes, était une demande ancienne de Bangui. En décembre 2017, la Russie adressa au Conseil de sécurité des Nations unies une demande d'exemption à l'embargo afin de pouvoir équiper deux bataillons des Forces armées centrafricaines (FACa). Placée sous « procédure de silence », cette requête put aboutir, la France, mais aussi les États-Unis et le Royaume-Uni, n'ayant pas manifesté leur opposition. Cette livraison d'armes aux FACa servit de prétexte à Moscou pour envoyer à Bangui des « instructeurs militaire civils », c'est-à-dire des mercenaires du groupe paramilitaire Wagner. La France s'est retirée de RCA et au plus fort, Wagner a rassemblé plus de 2 500 mercenaires dans le pays, même si la guerre en Ukraine a conduit la milice à réduire la voilure.

Progressivement, la France s'est trouvée complètement évincée de Centrafrique : Wagner a pris possession de l'ancien camp français et s'occupe également de la sécurité personnelle du Président Touadéra en lieu et place de l'armée française. Wagner forme également la police et la gendarmerie, ce qui lui donne accès à du renseignement. En contrepartie, Wagner a obtenu des engagements sur des mines d'or et de diamants.

Le 2 mars 2023, le Président Emmanuel Macron a rencontré son homologue Faustin Archange Touadéra à Libreville, en marge d'un sommet sur la préservation des forêts tropicales, ce qui n'a pas été du goût de Wagner, qui l'a fait savoir au Président centrafricain. Trois jours plus tard, à Doha, le Président Touadéra, lors de la Conférence des Nations-Unies sur les pays les moins avancés, dénonçait les ingérences étrangères et « *les pillages systématiques facilités par l'instabilité politique entretenue par certains pays occidentaux* ».

b. L'existence de liens historiques avec des puissances étrangères

Avant d'être élu en 2009 Président de l'Afrique du Sud, Jacob Zuma était en charge des services de renseignement de la branche armée de l'ANC. À l'époque où Vladimir Poutine était membre du KGB, Zuma avait été envoyé en Union soviétique pour se former. La dette morale de l'Afrique du Sud envers la Russie, très forte au vu de soutien que l'Union soviétique a apporté à la lutte contre l'Apartheid, explique aujourd'hui la proximité qui

existe entre les deux pays. Quand Serguei Lavrov, le ministre russe des affaires étrangères, est en visite en Afrique du Sud, il évoque « *l'ANC, grande amie de la Russie* ». On comprend mieux les abstentions répétées de l'Afrique du Sud lors des votes successifs aux Nations-Unies visant à condamner l'agression russe en Ukraine. Le pays, qui assure en 2023 la présidence tournante des BRICS (Brésil, Russie, Inde, Chine, Afrique du Sud) occupe une position stratégique qui rend d'autant plus problématique sa relation à Moscou, comme en témoignent les tergiversations sur la participation ou non de Vladimir Poutine au sommet des BRICS en août 2023 à Johannesburg.

La position à l'égard de la Russie est devenue un enjeu de politique intérieure en Afrique du Sud entre d'un côté l'ANC, le parti au pouvoir sans discontinuer depuis la fin de l'Apartheid et historiquement allié à la Russie et de l'autre le parti d'opposition *Democratic Alliance* (DA) qui dénonce cette proximité avec Moscou. À l'approche des élections législatives prévues en 2024, l'attention est portée sur une possible ingérence russe dans le processus électoral au vu de la forte probabilité pour l'ANC de perdre la majorité absolue qu'elle détient depuis son accession au pouvoir.

Le cas de **Madagascar** est lui aussi le reflet du poids de l'histoire et d'une relation ancienne avec Moscou. Les premières années qui suivirent la décolonisation sont restées marquées par une présence importante de la France que l'URSS n'avait de cesse de dénoncer, en particulier lors de la contestation étudiante de 1972. Jusqu'à l'effondrement de l'Union soviétique en 1991, Madagascar s'est alignée sur l'URSS, ce qui n'est pas sans laisser des traces.

Les relations actuelles entre Madagascar et la Russie sont pour le moins complexes. Il est établi que la Russie a tenté d'interférer dans le cours de l'élection présidentielle malgache de 2018. Une enquête du *New York Times* révèle en effet que le président sortant, Hery Rajaonarimampianina aurait demandé à la Russie de l'aider « *à résister aux tentatives des institutions internationales de s'immiscer* » dans les élections à Madagascar, visant vraisemblablement l'Union européenne qui avait dépêché une mission d'observation électorale. L'enquête du *New York Times* rapporte que les Russes ont lancé une campagne sur les réseaux sociaux et incité des candidats de faible envergure à se présenter pour diviser l'opposition. Cette opération d'ingérence, qui aurait coûté 16 millions d'euros, n'a toutefois pas eu l'effet escompté – Hery Rajaonarimampianina est éliminé dès le 1er tour – au point que la Russie a finalement décidé de se repositionner en faveur du candidat victorieux Andry Rajoelina.

À l'automne 2022, le pays s'est opposé à la venue sur l'île de Sergueï Lavrov et a aussi refusé l'escale d'une frégate russe à Diego Suarez. L'évolution des votes malgaches à l'ONU sur l'invasion russe en Ukraine est

également très instructive. D'une position de non alignement, Madagascar a opté en octobre 2022, à la surprise générale, pour la condamnation de l'agression russe ce qui a fait polémique dans l'opinion publique et suscité l'ire de Moscou, au point de provoquer le limogeage du ministre malgache des affaires étrangères au motif qu'il aurait agi sans l'aval du Président de la République ce qui, au vu du fonctionnement du pouvoir malgache, n'est pas crédible ; d'autant plus que Madagascar a réitéré en février 2023, un vote condamnant l'agression russe en Ukraine.

c. Un contexte géopolitique singulier

L'Afrique est depuis toujours le théâtre de rivalités entre grandes puissances. Après la décolonisation, pendant la guerre froide, Américains et soviétiques ont mené des guerres par procuration dans plusieurs pays du continent, contribuant à un accroissement de la taille des armées nationales et à une hausse des dépenses militaires et d'armement.

La lutte contre le terrorisme islamiste – *Aqmi*, *Daesh*, *Boko Haram* – au cœur des jeux de puissances étrangères, est entrée dans une phase nouvelle, dans le contexte de retrait des forces françaises et de redéploiement de Barkhane. Le G5 Sahel et ses États membres font face à une crise multidimensionnelle (sécuritaire, humanitaire, climatique) propice aux ingérences étrangères. Des groupes armés non étatiques planifient des attaques à grande échelle contre des cibles civiles et militaires et étendent leurs zones d'influence respectives pour contrôler les principales voies d'approvisionnement, tout particulièrement dans les zones frontalières entre le Burkina Faso, le Mali et le Niger.

Les enjeux géopolitiques mondiaux liés par exemple à l'exploitation des ressources naturelles, à la sécurité sanitaire – avec la diplomatie du masque –, à des prétentions territoriales (Taïwan) ou à des conflits armés (Ukraine) sont sans nul doute des faits générateurs d'ingérences étrangères.

L'analyse du vote qui s'est tenu le 2 mars 2022 à l'ONU sur la résolution condamnant la Russie pour l'invasion de l'Ukraine indique que sur les 35 pays qui se sont abstenus (sur 181 votants), 17 sont africains.

Sur un autre sujet, celui de Taïwan, on remarquera que parmi les treize pays au monde qui reconnaissent officiellement Taïwan, un seul est africain : il s'agit de l'Eswatini (anciennement nommé Swaziland). Cette monarchie enclavée, située entre l'Afrique du Sud et le Mozambique, a été frappée en 2021 par des troubles liés à des manifestations qui ont dégénéré dans le sang et plongé le pays dans un climat de quasi guerre civile. Les pays de la SADC, réunis en sommet en janvier 2023 en Namibie ont exprimé leur préoccupation sur « *l'escalade des tensions* » en Eswatini dont on ne peut exclure que la

Chine ait, d'une façon ou d'une autre, joué un rôle pour déstabiliser ce petit royaume favorable à Taïwan.

2. La mise au jour de véritables stratégies d'ingérence

a. Les signaux faibles prémisses de futures ingérences

À l'aéroport de Johannesburg, des exemplaires du magazine « ChinAfrica » sont distribués gratuitement aux voyageurs qui arrivent dans le pays. Imaginerait-on un seul instant un magazine intitulé « Françafrique » ? Cela en dit long de l'approche décomplexée qui est celle des deux principales puissances étrangères – La Chine et la Russie – qui investissent le continent africain à travers des leviers d'action susceptibles de participer à la mise en place de possibles ingérences futures.

On constate ces derniers temps une accumulation de signes avant-coureurs d'une préparation des terrains informationnel, politique et économique de la part de la Russie, notamment *via* des entités parapubliques liées à Evgueni Prigojine, le fondateur du groupe Wagner. En Afrique, les **modes opératoires caractéristiques** de la Russie sont les suivants :

– **La propagande** : Bannie en Europe à cause de la guerre en Ukraine, la chaîne de télévision *Russia Today*, principal rouage de la machine de propagande du discours russe, vient de choisir l'Afrique du Sud pour installer les bureaux de sa plateforme anglophone sur le continent africain.

– **Les ventes d'armes** : la Russie est le premier vendeur d'armes en Afrique subsaharienne, passant devant la Chine. Cela n'est pas sans lien avec l'implantation des sociétés militaires privées telles Wagner. Entre 2018 et 2022, les ventes d'armes russes y ont représenté 26 % de parts de marché contre 18 % pour la Chine, 8 % pour la France et 5 % pour les États-Unis, selon les chiffres publiés par l'Institut international de recherche sur la paix de Stockhom (Sipri).

– **La formation des forces de sécurité** à travers la conclusion d'accords de coopération militaire. Moscou cherche à nouer des partenariats sécuritaires avec le plus de pays possibles en Afrique. L'accord signé en 2022 avec Madagascar porte notamment sur la formation des officiers malgaches, le transfert d'expertise ou encore le renouvellement des armes. En avril 2023, un accord de défense a été signé entre la Russie et le Cameroun, signe supplémentaire de la perte d'influence de la France en Afrique francophone. En mai 2023, le chef de l'armée sud-africaine a rencontré son homologue russe à Moscou quelques jours à peine après que les États-Unis ont accusé

l'Afrique du Sud d'avoir livré clandestinement des armes à la Russie [(1)]. La réunion entre les commandants militaires russe et sud-africain a débouché sur des accords concernant le développement de la coopération entre les forces terrestres des deux pays. Déjà en février 2023, des manœuvres navales entre l'Afrique du Sud, la Russie et la Chine s'étaient déroulées au large des côtes sud-africaines, en pleine commémoration du premier anniversaire du déclenchement de la guerre en Ukraine.

– **L'investissement dans le secteur minier,** notamment par l'intermédiaire de sociétés militaires privées qui assurent la sécurisation des sites. Wagner a ainsi investi 65 millions d'euros dans une mine de chrome à Madagascar, à travers la société *Ferrum Mining* mais l'exploitation de la mine est à l'arrêt depuis 2019 en raison de divergences entre les actionnaires.

S'agissant de la Chine, les modes opératoires sont différents et relèvent davantage du champ économique, des outils de *soft power* et aussi, de plus en plus, des instruments de coopération militaire. On peut ainsi évoquer :

– **L'investissement dans les infrastructures** (BTP, routes, ports, chemins de fer, énergie), véritable signature de la présence chinoise qui déploie en Afrique sa stratégie des nouvelles routes de la soie (*Belt and Road Initiative*). À Madagascar, les opérateurs chinois sont ainsi présents dans quatre secteurs extractifs clés pour l'économie malgache : pêche, bois, mine et hydrocarbures. La Chine déploie également un projet majeur d'investissement de construction d'un port en eaux profondes à Narindra, sur la côte ouest de Madagascar et qui n'est pas neutre d'un point de vue stratégique, compte tenu de son possible usage militaire.

– La présence dans le secteur bancaire est une orientation stratégique des autorités chinoises. La banque industrielle et commerciale de Chine (ICBC) détient ainsi 20 % de *Standard Bank*, la plus importante banque sud-africaine, présente dans une vingtaine de pays africains.

– **Le *soft power*, à travers les Instituts *Confucius***, au nombre de 61 dans 41 pays africains ainsi que sur l'île de la Réunion. Les autorités chinoises sont en alerte permanente sur toute activité susceptible de nuire à ses intérêts. Un membre de l'Ambassade de Chine en Afrique du Sud a ainsi ouvertement reproché à une université de Pretoria d'avoir laissé un de ses chercheurs donner une conférence sur les relations entre la Chine et Taïwan dans les locaux du Bureau de Représentation de Taïwan.

---

(1) En janvier 2023, un navire marchand russe, le Lady R, dont le propriétaire aurait transporté des armes pour le Kremlin a éteint son transpondeur avant d'accoster subrepticement à la plus grande base navale d'Afrique du Sud, où il a livré et chargé des cargaisons non identifiées.

– **La multiplication des accords de coopération militaire** conclus par la Chine avec différents pays africains. Les Chinois expriment également leur volonté de participer à des opérations de maintien de la paix sous mandat de l'ONU sur le continent africain.

Derrière ces actions à visage découvert, on observe également des stratégies plus dissimulées susceptibles de nourrir de possibles ingérences. C'est ainsi que l'action des services de renseignement a permis de caractériser le recrutement par l'Afrique du Sud d'ancien pilotes occidentaux disposants de savoir-faire de l'OTAN qui ensuite, formaient à leur tour des pilotes chinois ; ces formations à rebonds auraient ainsi permis à la Chine d'accéder à des savoir-faire protégés. Pour former les pilotes de son armée de l'Air, la Chine recrute en effet d'anciens pilotes de chasse Français, Britanniques, Américains et Allemands *****.

b. Vers une convergence des ingérences

Parce que l'ennemi de mon ennemi est mon ami, il est des stratégies isolées qui peuvent à un moment donné se retrouver pour converger autour d'intérêts communs. Depuis Madagascar, un axe entre la Russie et l'Iran est ainsi en train de se mettre en place pour déstabiliser le pouvoir aux Comores et par là-même porter atteinte aux intérêts français dans la zone.

L'ambassade de Russie à Madagascar aurait ainsi été à l'origine d'une rencontre à Antananarivo entre Hamada Madi Bolero, conseiller diplomatique du Président comorien Azali formé en Russie, et l'ambassadeur d'Iran. Quelques semaines plus tard, le 3 juin 2023, les Comores – qui exercent la présidence tournante de l'Union Africaine – ont officiellement demandé la reprise des relations diplomatiques avec la République islamique d'Iran, rompues en 2016 pour cause d'ingérence de l'Iran dans la politique intérieure de certains États.

La mise en place de cet axe Moscou – Téhéran aux Comores n'est pas sans conséquence sur le renforcement de la présence américaine dans la zone qui n'entend pas laisser le champ libre aux Russes et aux Iraniens. Il serait néanmoins regrettable que la France devienne le parent pauvre d'une compétition entre la Russie et les États-Unis comme au plus fort de la guerre froide.

B. LA CONTESTATION DES INTÉRÊTS FRANÇAIS DANS LA RÉGION PREND DES FORMES MULTIPLES

Les intérêts français en Afrique australe et dans l'océan indien sont multiples et revêtent une dimension stratégique. L'action des services de

renseignement français – principalement la DTSI pour les départements d'outre-mer et la DGSE pour l'étranger – consiste à identifier et à neutraliser les actions de déstabilisation qui ciblent notre pays en contestant la présence française, jusqu'à la remise en cause notre souveraineté sur certains territoires de l'océan indien.

1. La contestation de la présence française

La **tentation francophobe** prend différentes formes : opérations de manipulation de l'information visant à porter atteinte à l'image et à la réputation de la France, procès politiques, actions hostiles aux entreprises françaises et à nos intérêts économiques.

En Afrique du Sud, L'*Economic Freedom Fighters* (EFF) est un parti politique fondé en 2013 par d'anciens membres dissidents de l'ANC et dont le score progresse à chaque élection. Ce parti soutient officiellement l'invasion de l'Ukraine par la Russie, au titre de l'anti-impérialisme de la Russie contre l'OTAN. Il est clairement un relais des intérêts russes à travers des opérations de déstabilisation visant l'Occident.

L'EFF est ainsi à l'origine d'une manifestation anti-française le 25 mai 2022 devant l'ambassade de France à Pretoria dont l'objet visait à demander tout simplement de départ de la France du continent africain. Des centaines d'affiches anti-françaises d'appel à cette manifestation furent placardées partout dans la ville grâce à un soutien financier et logistique manifeste. *****

Dans un autre registre, au titre des procès intentés à des ressortissants français, le cas de Philippe François, dirigeant d'une société d'investissement à Madagascar, est emblématique. Cet ancien saint-cyrien, colonel de l'armée française jusqu'en 2013, est accusé, avec le franco-malgache Paul Rafanoharana, d'avoir voulu renverser et assassiner l'actuel président de Madagascar, Andry Rajoelina. Dans ce dossier baptisé « Apollo 21 » par les autorités malgaches, 21 personnes ont été poursuivies et jugées pour atteinte à la sûreté de l'État, association de malfaiteurs et complot en vue d'assassiner le président. Selon la procureure générale, ils auraient échafaudé un plan d'élimination et de neutralisation de diverses personnalités malgaches dont le chef de l'État. Le procès s'est tenu fin 2021 et à l'été 2022, la Cour de cassation de Madagascar a confirmé la peine de dix ans de travaux forcés infligée à l'ancien militaire français, décoré de la croix de la Valeur militaire et de la croix de guerre des théâtres d'opérations extérieures et qui a servi 25 ans dans les troupes de marine.

Son incarcération, dans les conditions que l'on imagine, n'a pas été de nature à apaiser les relations franco-malgaches marquées par la revendication historique de Madagascar sur les îles éparses dont Antananarivo exige la restitution depuis 1973. Philippe François a finalement pu être transféré en France le 23 juin 2023.

Cette affaire n'est pas un cas isolé en Afrique et la France est régulièrement accusée, directement ou indirectement, de soutenir des actions de déstabilisation. En Centrafrique, l'attaque au colis piégé perpétrée le 16 décembre 2022 contre Dimitri Sytyi, chef du centre culturel russe à Bangui, a conduit Wagner à qualifier la France « *d'État soutien du terrorisme* » et à considérer que cet acte criminel visait à nuire aux bonnes relations entre Moscou et Bangui. Toujours en Centrafrique, notre ressortissant Juan Rémy Quignolot, accusé d'espionnage, a passé seize mois en détention préventive à Bangui avant d'être remis en liberté sous contrôle judiciaire en septembre 2022 et assigné à résidence à l'ambassade de France à Bangui. Cet ancien militaire reconverti dans la sécurité et la formation à la lutte contre le braconnage, a finalement pu être rapatrié en France le 21 mai 2023, pour raisons de santé, mais devra retourner à Bangui pour la tenue de son procès.

Tout ceci participe d'une propagande anti-française qui cible également nos intérêts économiques. Dans la nuit du 6 mars 2023, des engins incendiaires ont été utilisés pour mettre le feu à la brasserie Motte Cordonnier Afrique (Mocaf). Présente en Centrafrique depuis 1953 et acquise en 1993 par Castel, cette filiale est l'un des plus gros producteurs et employeurs du pays. Mais Wagner a ouvert fin 2021 sa propre brasserie à Bangui pour concurrencer les Français, avec le lancement d'une nouvelle boisson, l'*Africa ti l'or*, sur le marché centrafricain. *****

Cet incendie criminel de la brasserie Mocaf qui est intervenu quelques jours à peine après la rencontre entre les présidents Macron et Touadéra, est aussi une illustration emblématique de la guerre d'influence qui se joue en Centrafrique où la Russie voit d'un très mauvais œil un possible rapprochement entre Bangui et Paris. Dans le cadre de l'opération Sangaris, la France avait déployé entre 2013 et 2016 jusqu'à plus de 1 500 soldats en Centrafrique avant que les troupes françaises ne se retirent dans un contexte d'une présence grandissante du groupe paramilitaire Wagner dans le pays qui avait conduit le Président Macron à dénoncer au printemps 2021 ces *« mercenaires prédateurs russes au sommet de l'État avec un président Touadéra qui est aujourd'hui l'otage du groupe Wagner ».*

2. La contestation de la souveraineté française

Après les États-Unis, la France dispose de la deuxième zone économique exclusive (ZEE) la plus importante au monde, d'une superficie supérieure à dix millions de km². Notre présence dans l'océan indien constitue 93 % de la ZEE de la France. Si les îles de la Réunion et de Mayotte sont les plus connues, certains territoires, habités ou non, font l'objet de contentieux anciens entre la France et plusieurs États que sont notamment Maurice (Tromelin) et Madagascar (îles Éparses). La situation à Mayotte est également un sujet de tension majeur entre la France et les Comores comme l'a illustré l'opération Wuambushu lancée en mai 2023. Ces contentieux et ces tensions sont régulièrement instrumentalisés par des puissances étrangères qui les utilisent pour nuire à nos intérêts fondamentaux.

Hormis les scientifiques et militaires, **les îles Éparses** dont la plupart sont situées dans le canal du Mozambique, demeurent inhabitées la majeure partie du temps. Depuis 1973, la souveraineté française sur les îles Éparses est principalement assurée par la présence militaire des forces armées dans la zone sud de l'océan Indien (FAZSOI) ; en 2005, elles sont passées sous l'autorité des Terres australes et antarctiques françaises (TAAF).

Une résolution – non contraignante – des Nations Unies de 1979 invite la France à restituer les îles Éparses à Madagascar ou, *a minima*, à entamer des négociations. En 2019, le Président Emmanuel Macron s'est dit ouvert au dialogue et disposé à trouver une solution commune. Une commission mixte sur les îles Éparses fut alors mise en place et s'est réunie une première fois en novembre 2019 avec l'ambition d'aboutir à cette solution commune, idéalement pour du 60e anniversaire de l'indépendance de Madagascar, le 26 juin 2020. Mais la crise du Covid a contrarié ce calendrier. Une nouvelle réunion de la commission mixte fixée en septembre 2022 a dû être annulée au dernier moment en raison du limogeage du ministère malgache des affaires étrangères à la suite du vote aux Nations Unies de la résolution condamnant l'invasion russe en Ukraine. Faute de convocation de la commission mixte, les discussions sont à ce jour au point mort et certaines puissances étrangères comme la Russie, ne manquent pas une occasion de rappeler leur soutien à la revendication de Madagascar sur les îles Éparses.

L'ambassade de Russie à Madagascar mène une offensive diplomatique. Dans un message adressé aux participants à l'Assemblée générale de l'association des Amis de Russie à Madagascar, l'ambassadeur de la Fédération de Russie, Andrey Andreev, a réitéré le soutien de la Russie face à la volonté légitime de la République de Madagascar de se voir restituer les îles Éparses sous sa souveraineté.

Aux Comores aussi, la Russie n'hésite pas à jouer des tensions liées à la situation à Mayotte, allant même jusqu'à se prononcer en faveur d'une « Mayotte comorienne ». Recevant à Moscou en novembre 2018 le ministre comorien des affaires étrangères, Serguei Lavrov a affirmé que « *Malgré de nombreuses résolutions adoptées par l'Assemblée Générale de l'ONU sur cette question, la France continue à détenir Mayotte d'une façon illégitime* ».

À l'approche du déclenchement de l'opération Wuambushu, la France a été la cible d'une campagne anti-française sur les réseaux sociaux qui a coïncidé avec la visite de l'ambassadeur russe à Moroni. Un « influenceur » comorien, au pseudo de « Nono » a fait son apparition, postant des messages anti-français. Dans le même temps, des drapeaux russes étaient brandis dans des manifestations anti-françaises à Moroni. *****

À LA RÉUNION, L'ACTION DE L'ANTENNE DE LA SÉCURITÉ INTÉRIEURE POUR PRÉVENIR ET ENTRAVER LES INGÉRENCES ÉTRANGÈRES

À Saint-Denis de la Réunion, *****

C. ORIENTER NOTRE OUTIL DE RENSEIGNEMENT DANS UNE STRATÉGIE DE RIPOSTE AUX INGÉRENCES ÉTRANGÈRES HOSTILES

Face aux ingérences étrangères qui visent les intérêts français, nos services de renseignement agissent, seuls ou en lien avec d'autres acteurs, de multiples façons pour prévenir, détecter, suivre et entraver.

Il s'agit d'une part d'ouvrir tous nos capteurs de renseignement pour identifier et exploiter les faiblesses de nos adversaires et d'autre part, la nature ayant horreur du vide, d'occuper le terrain quand il n'est pas trop tard, là où c'est encore possible.

1. Renseigner pour mieux exploiter les faiblesses de nos adversaires

Face à l'offensive de puissances étrangères – essentiellement la Russie et la Chine – pour affaiblir notre présence et nuire à nos intérêts, le renseignement peut et doit davantage être mis à profit pour capter des informations sur les faiblesses de nos adversaires, à charge ensuite d'en assurer la meilleure exploitation possible.

Car derrière les apparences, la Russie et la Chine sont loin d'être en terrain conquis dans les pays qu'ils investissent. Les vulnérabilités de nos adversaires sont les suivantes :

– Tout en accusant l'occident de néocolonialisme, la Russie et la Chine se comportent en réalité comme des prédateurs, pillant les ressources naturelles des pays qu'ils exploitent, peu scrupuleux avec le respect de l'environnement exerçant leur mainmise sur la souveraineté même de ces États. C'est en particulier le cas des chinois qui ont réalisé de grands projets d'infrastructures moyennant des prêts remboursés en or, en pétrole ou en gaz. En République Démocratique du Congo, un rapport de l'Inspection générale des finances a dénoncé les déséquilibres du méga contrat minier signé en 2008 avec des partenaires chinois, lesquels ont très largement sous-évalué le montant qu'ils devaient reverser au gouvernement congolais. La mine a été mise à l'arrêt pendant un an, le temps de renégocier ledit contrat. Les entreprises chinoises auraient en effet engrangé dix milliards de dollars alors que leurs investissements dans les infrastructures sont évalués à 833 millions de dollars depuis 2008.

– Ces puissances étrangères ne contribuent en rien à dynamiser l'économie des pays concernés ; au contraire, la violence à l'égard des populations locales est de mise, assortie de racisme et qui s'accompagne d'un sentiment d'abandon des populations locales.

– Wagner subit des échecs, notamment au Mozambique, où la milice paramilitaire a dû reculer au bout de deux mois face au groupe armé État islamique (EI). Plus grave encore, le désordre, l'insécurité et la crise servent Wagner qui n'a pas intérêt à régler les conflits au risque de réduire à néant son utilité présumée.

Au final, il y a un front réputationnel à ouvrir et à nourrir sur le fondement de renseignements précis à collecter sur les vulnérabilités russes et chinoises et l'image négative qu'ont ces pays auprès des populations locales. L'enjeu n'est pas seulement de détecter les faiblesses et de fournir du renseignement, mais bien d'**exploiter ce renseignement de façon appropriée et réactive**. Cela suppose d'intégrer le renseignement dans un cercle vertueux de la riposte qui s'appuie aussi sur les médias et les réseaux sociaux. **(Recommandation n° 18)**

Il est frappant d'observer, dans une époque où les rapports de force et les conflits sont désormais hybrides, à quelle vitesse les renseignements sont rendus publics. Les Américains eux-mêmes n'hésitent pas à déclassifier des renseignements : ils l'ont fait sur le Covid comme sur la guerre en Ukraine. Le renseignement devient une arme à part entière pour exploiter au mieux les failles de ceux que l'on combat.

2. Occuper le terrain

Parce que la nature a horreur du vide, il est nécessaire de mieux valoriser et d'amplifier l'action de la France dans les pays où nous sommes présents, au même titre qu'il importe de communiquer davantage sur les faiblesses de nos adversaires.

En d'autres termes, il s'agit de **rendre la marche plus haute pour ceux qui voudraient nuire à nos intérêts**. Nous disposons d'atouts solides et nous pouvons nous appuyer sur notre *soft power* à travers un réseau d'établissements scolaires et d'alliances françaises d'une densité remarquable. L'action de la France s'agissant de l'aide au développement est également à mettre à notre crédit : à Madagascar, par exemple, les engagements de l'Agence française de développement (AFD) représentent à eux seuls près de 400 millions d'euros.

a. Le projet de base de l'action de l'État en mer porté par la France à Diego-Suarez

Le projet de création d'une **base de l'action de l'État en mer à Antsiranana (Diégo-Suarez)** est de nature à ancrer la présence et l'influence française, potentiellement concurrencée par des projets d'envergure d'autres nations qui pourraient y développer une présence stratégique.

La base navale d'Antsiranana est l'héritage de la présence de la marine française à Madagascar. Mais depuis 1970, aucun investissement n'y a été effectué. Les bâtiments de la Marine nationale française effectuent chaque année une dizaine de relâches opérationnelles. Les équipages français sont ceux qui s'ouvrent le plus à la population locale quand certains équipages étrangers à Madagascar ne quittent même pas leur bord. Ceci participe au maintien d'un sentiment francophile à Antsiranana, mais néanmoins fragile.

Or le Gouvernement malgache est à la recherche d'un partenaire pour développer un projet de ville nouvelle au nord d'Antsiranana sur la presqu'île d'Andrakaka. Sur de vastes terrains, aujourd'hui à l'usage des armées, il s'agirait de construire un port en eaux profondes, des complexes hôteliers, une zone industrielle, une route d'accès de 55 kilomètres… À ce jour, le besoin de financement pour ce projet majeur est évalué à deux milliards de dollars et la Chine se positionne pour un probable bailleur. Les Russes également semblent montrer un intérêt pour cette zone avec l'escale en 2019 d'un bâtiment militaire russe.

*****

b. L'identification de nouveaux partenaires

Il existe en Afrique Australe un certain nombre de pays qui sont en demande de coopérer davantage avec la France. Certes, ces pays ne sont pas dans notre zone historique d'influence ; mais c'est justement là notre intérêt de nous ouvrir à eux sans porter le poids de notre passé colonial. Avec le Brexit, il faut faire preuve de pragmatisme envers des pays comme le Zimbabwe avec lesquels il y a une carte à jouer si nous ne voulons pas laisser le champ libre à la Russie ou à la Chine. Car si nous n'y allons pas, d'autres iront évidemment à notre place.

Il importe ainsi d'identifier les États avec lesquels nous pourrions développer des coopérations en matière de sécurité et de renseignement. **(Recommandation°19)**

*****

3. Renforcer notre dispositif de renseignement

À la lumière de l'intensification des ingérences étrangères qui menacent directement nos intérêts, la Délégation estime nécessaire de **réévaluer les moyens du renseignement français** en Afrique australe et dans l'océan indien.

*****

Nonobstant la réorientation de nos capteurs de renseignement vers la Chine, l'indopacifique mais aussi l'Europe du fait de la guerre en Ukraine, ***** Plusieurs raisons vont dans ce sens :

– L'Afrique du Sud fait partie des BRICS, ce qui confère à la zone un intérêt stratégique car le pays entretient des relations institutionnalisées avec la Russie et la Chine. *****

– L'Afrique australe est une zone qui fait office de plaque tournante s'agissant de nombreux trafics vers l'Europe, notamment de stupéfiants.

Il s'agit d'une alternative nécessaire à notre zone d'influence historique de l'Afrique francophone.

***** **(Recommandation°20)**

Le renforcement de nos moyens concerne également notre présence dans l'océan indien. ***** **(Recommandation°21)**

Enfin, même s'il ne s'agit pas de renseignement à proprement parler, il serait judicieux de repenser notre dispositif de coopération. Le nombre de coopérants français n'a cessé de diminuer au cours des dernières années, marqueur de la volonté politique de tourner la page de la françafrique. Pour autant, dans le contexte d'intensification des ingérences étrangères, les coopérants sont des relais privilégiés qui contribuent utilement à une stratégie d'influence. Dans l'hypothèse de relations nouvelles avec certains pays d'Afrique, comme le Malawi, le dispositif de la coopération pourrait se révéler approprié. **(Recommandation°22)**

***

CHAPITRE IV :
RAPPORT GÉNÉRAL DE LA CVFS

sur les conditions d'emploi des fonds spéciaux au cours de l'exercice 2021

Le contrôle de l'utilisation des fonds spéciaux a été confié par le législateur (loi de finances pour 2002) à la commission de vérification des fonds spéciaux (CVFS), dont la composition a été modifiée par la loi de programmation militaire du 18 décembre 2013 qui en fait une formation spécialisée de la délégation parlementaire au renseignement (DPR).

La CVFS, composée de deux députés et deux sénateurs membres de la DPR est chargée de « *s'assurer que les crédits [en fonds spéciaux] sont utilisés conformément à la destination qui leur a été assignée par la loi de finances* ».

Au mois de janvier 2022, sa composition était la suivante :

– M. Loïc Kervran, député (Agir ensemble) du Cher, président ;

– Mme Agnès Canayer, sénateur (Les Républicains) de la Seine-Maritime ;

– M. Claude de Ganay, député (Les Républicains) du Loiret ;

– M. Yannick Vaugrenard, sénateur (Socialiste, Écologiste et Républicain) de la Loire-Atlantique.

À la suite des élections législatives de juin 2022, la CVFS a été profondément renouvelée. À compter du mois de juillet, la commission était composée comme suit :

– M. Yannick Vaugrenard, sénateur (Socialiste, Écologiste et Républicain) de la Loire-Atlantique, président ;

– Mme Agnès Canayer, sénateur (Les Républicains) de la Seine-Maritime ;

– Mme Caroline Colombier, députée (Rassemblement National) de la Charente ;

– Mme Constance Le Grip, députée (Renaissance) des Hauts-de-Seine.

Pour mener sa mission et réaliser son rapport, la CVFS s'est déplacée au siège de chacune de structures bénéficiaires de fonds spéciaux pour y réaliser des contrôles sur place et sur pièces.

Elle s’est ainsi rendue :

– à la direction générale de la sécurité extérieure (DGSE), les 9, 12 et 31 mai, 2 et 9 juin, 28 septembre, 14 et 20 octobre et 17 novembre 2022 ;

– à la direction générale de la sécurité intérieure (DGSI), les 14 septembre et 2 novembre 2022 ;

– à la direction du renseignement militaire (DRM), les 25 octobre, et 4 et 14 novembre 2022 ;

– à la direction du renseignement et de la sécurité de la défense (DRSD), les 24 mai et 13 septembre 2022 ;

– à la direction nationale du renseignement et des enquêtes douanières (DNRED), les 1er juin et 18 octobre 2022 ;

– à Tracfin, les 24 mai et 27 septembre 2022 ;

– au service national du renseignement pénitentiaire (SNRP), les 27 avril et 27 septembre 2022 ;

– au groupement interministériel de contrôle (GIC), les 20 septembre et 28 novembre 2022.

Au cours de ces visites, la commission a auditionné les principaux responsables des services et a systématiquement procédé à un contrôle par échantillonnage des pièces comptables.

En raison du contexte sanitaire, d’une part, et du calendrier électoral, d’autre part, elle n’a pu se déplacer auprès de postes à l’étranger pour y effectuer des contrôles.

*

* *

I. LA PRÉSENTATION GÉNÉRALE DES FONDS SPÉCIAUX EN 2021

L'exercice 2021 se caractérise par **une réduction significative des trois principaux indicateurs de suivi de la gestion des fonds spéciaux**, à savoir :

– une **baisse des dotations en fonds spéciaux de près de 6,5 % (*****) en 2021**, après transferts et redéploiements) par rapport à 2020 (*****) ;

– une **réduction de près de 5 % des dépenses**, dont le montant en 2021 a représenté ***** M€ en 2020 ;

– la **poursuite de régulation à la baisse de la trésorerie globale des services de renseignement**, *****.

Il s'agit de **trois tendances globales qui ne doivent toutefois pas masquer des disparités importantes entre les neuf services contrôlés**, notamment entre les trois principaux services dépensiers ***** et les autres services *****qui, au contraire, ont connu une montée en puissance ***** des dépenses (*cf. infra*).

Enfin, il convient de souligner le **caractère transitoire de ces tendances** dans la mesure où la modération observée en 2021 sur les ressources et les dépenses correspond, d'une part, à une année de reprise partielle d'activité post-covid, et d'autre part, à un début de mise en œuvre des plans d'apurement et de régulation des trésoreries excédentaires recommandés par la CVFS.

*****. À cet égard, la CNRLT présente une **prévision de régulation du niveau global de trésorerie** *****. Cette cible constituera donc un point de vigilance à suivre par la CVFS. Enfin, le chapitre des dépenses constitue l'autre caractère transitoire de l'année 2021, car dès 2022, année pleine post-covid marquée par la guerre en Ukraine notamment, **la CNRLT prévoit un ressaut important des dépenses**, *****.

A. UN AJUSTEMENT À LA BAISSE DES DOTATIONS EN FONDS SPÉCIAUX POUR LES TROIS PRINCIPAUX SERVICES *****

De 66,80 M€ en 2019, puis 76,36 M€ en 2020, la dotation initiale globale des services de renseignement contrôlés s'est établie à 75,98 M€ en 2021.

*****

Au total, les ressources allouées en 2021, après abondements, se sont élevées à *****

Par ailleurs, aucun décret pour dépenses accidentelles et imprévisibles (DDAI) n'a été pris sur la période, les redéploiements ***** ayant suffi à pourvoir aux besoins supplémentaires *****.

Il convient ainsi de souligner que l'allocation en 2021 des fonds spéciaux s'est inscrite, sans l'excéder, dans le montant voté en loi de finances initiale au programme 129 « Coordination du travail gouvernemental ». Ce n'était pas le cas les années précédentes.

Toutefois, si la question de la sincérité budgétaire s'apprécie à l'aune des transferts ou redéploiements récurrents qui viendraient altérer la sincérité de la prévision budgétaire, elle s'apprécie en priorité au regard des dépenses exécutées. *****

La politique d'apurement des excédents de trésorerie justifie que les résultats d'exercice soient négatifs un temps – le temps d'atteindre un niveau de fonds de roulement adapté *****–, mais devra se poser à partir de 2023, pour le projet de loi de finances pour 2024, la question de la réévaluation des crédits en fonds spéciaux du programme 129 précité, à la hauteur des dépenses effectives.

B. UN TROISIÈME EXERCICE CONSÉCUTIF DE RÉDUCTION DU MONTANT GLOBAL DES DÉPENSES

1. La réduction des dépenses ***** justifie, à elle seule, la baisse ***** des fonds spéciaux dépensés *****

*****, il s'agit de la troisième année consécutive de baisse globale des dépenses en fonds spéciaux – *****.

Cette baisse est intégralement à mettre à l'actif de la réduction de ***** des dépenses *****. L'ensemble des autres services ont vu leurs dépenses augmenter, de manière modérée ***** ou beaucoup plus significative ***** (*cf.* tableau ci-après). L'ensemble de ces « petits » services, *****, suivent des politiques de renforcement de leurs actions et de leurs structures.

ÉVOLUTION DES DÉPENSES EN FONDS SPÉCIAUX (EN M€)

*****

2. Une sincérité budgétaire remise en cause en 2022 et à remettre à niveau par les services du Premier ministre pour les exercices suivants

Il est à noter qu'à l'exception *****, l'ensemble des prévisions de dépenses va augmenter en 2022 et les années suivantes, notamment au sein de *****

Par ailleurs, compte tenu du niveau des dépenses d'ores et déjà prévu pour 2022, la CVFS constate que les crédits en fonds spéciaux prévus par le programme 129 « Coordination du travail gouvernemental » de la mission budgétaire « Direction de l'action du Gouvernement » sont notoirement sous-budgétés, leur montant s'établissant à 76 M€ pour 2023, inchangé depuis 2020. **La sincérité de la budgétisation des lois de finances initiales devra donc faire l'objet d'une sérieuse remise à niveau** à l'occasion de la discussion des prochaines lois de finances rectificatives et lois de règlement des comptes de l'année 2022. En effet, **le décalage entre le montant budgété en loi de finances initiale (76 M€) et la prévision de dépenses ***** est trop patent pour ne pas justifier un meilleur dialogue entre la CNRLT et le cabinet de la Première ministre**.

Bien que le détail de la ventilation des fonds spéciaux par service bénéficiaire soit classifié, **les documents budgétaires doivent au moins permettre d'assurer la transparence de l'enveloppe globale des fonds spéciaux, tant en budgétisation qu'en exécution.**

3. L'analyse des typologies de dépenses fait de 2021 une année atypique

Selon les prévisions fournies par la CNRLT, le niveau des dépenses de l'année 2021 devrait constituer l'étiage – le creux de la courbe – avant une remontée en 2022. On observe ainsi que *****

C. UNE RÉGULATION INÉGALE DU NIVEAU DE TRÉSORERIE IMMOBILISÉE, GAGÉE ET DISPONIBLE

La CVFS avait reconduit et précisé, sur la base du contrôle de l'exercice 2020, la recommandation visant à lancer un programme d'apurement et de régulation des réserves de trésorerie jugées excessives, *****

Dans ces conditions, la persistance d'un résultat d'exercice négatif pour l'année 2021 – c'est-à-dire des dépenses non intégralement couvertes par la dotation – pouvait utilement concourir à la consommation des fonds non indispensables à la tenue d'un fonds de roulement suffisant pour assurer la solvabilité du service dans sa gestion courante. *****

Le déficit du résultat d'exercice a participé à la réduction souhaitée par la CVFS du montant total des différentes trésoreries. *****

La CVFS salue notamment la réduction très significative *****

II. LES OBSERVATIONS COMMUNES À L'ENSEMBLE DES SERVICES

L'examen des comptes en fonds spéciaux de l'ensemble des services bénéficiaires permet à la CVFS de disposer d'une vision globale et transversale de leur gestion.

S'il existe des spécificités propres à chaque structure, il n'en demeure pas moins que des réflexions et des problématiques communes conduisent la commission à formuler un certain nombre d'observations générales issues des contrôles sur pièces et sur place, effectués au titre du contrôle sur l'exercice 2021.

Comme l'année dernière, la commission salue des progrès sur plusieurs sujets, s'agissant notamment de la montée en puissance et de la maturité des procédures de contrôle interne.

Des évolutions positives sont également constatées en matière *****, ou encore de la diffusion de plus en plus large d'une culture sur l'usage des fonds spéciaux au sein des services de renseignement, à l'échelon central comme dans les implantations territoriales et dans nos postes à l'étranger.

A. LA NÉCESSITÉ D'UNE APPLICATION STRICTE DE LA DOCTRINE D'EMPLOI FACE À L'AUGMENTATION TENDANCIELLE DES FONDS SPECIAUX

Cependant deux phénomènes, l'un conjoncturel, l'autre durable, appellent l'attention de la commission.

Le phénomène conjoncturel réside dans le montant important ***** au sein de plusieurs services. Cette situation est susceptible de se résoudre dès 2022, en raison de l'augmentation de l'activité des services, mais elle appelle l'attention des services et de la coordination nationale.

La tendance structurelle réside, quant à elle, dans l'augmentation des dépenses en fonds spéciaux, les services les plus dotés voyant une augmentation

de leurs effectifs et de leurs missions, et les services les moins dotés étant appelés à monter rapidement en charge.

Cette augmentation en l'espace de quelques années rend d'autant plus nécessaire l'application de la doctrine élaborée par la CVFS sur l'usage des fonds spéciaux – qui limite le recours à ces fonds à la nécessité de confidentialité ou l'urgence –, ainsi que la mise en place de mécanismes incontestables permettant d'assurer leur contrôle. Le processus de « fonds-normalisation » des dépenses ne répondant pas aux critères d'emploi des fonds spéciaux, déjà engagé par les services, doit être poursuivi et mené le plus rapidement possible à son terme. De nombreuses possibilités, *****, sont encore sous-employées *****

La CVFS a toujours soutenu l'adéquation des dotations accordées au service à leurs missions, et l'extension de celles-ci. Cependant, les fonds spéciaux ne peuvent en aucun cas servir de facilité pour contourner les complexités administratives, ou d'appoint pour faire face aux insuffisances de crédits généraux.

L'extension du recours aux fonds spéciaux appelle aussi un regard de la coordination nationale sur la conformité des usages aux missions de services *****

B. LE POIDS PARFOIS DISPROPORTIONNÉ DES FRAIS BANCAIRES SUPPORTÉS PAR LES SERVICES

Cette année, la CVFS a été amenée à se pencher, de nouveau, sur la question des frais bancaires supportés par les services, tant au titre des frais fixes que des intérêts négatifs. Si cette dernière difficulté, ***** est appelée à disparaître avec l'évolution des taux d'intérêt, la première demeure.

En effet, les frais fixes facturés par la Banque de France, importants en valeur absolue pour tous les services, pèsent plus que proportionnellement sur les services les moins dotés. *****

Faute de progrès sur la question ancienne des relations financières avec la Banque de France, la commission avait éteint, en 2020, sa recommandation émise en 2015. Au regard des difficultés nouvelles rencontrées, la CVFS souhaite que la CNRLT se rapproche de la Banque de France afin que les frais bancaires supportés par les services puissent faire l'objet de l'évaluation la plus juste possible.

Recommandation générale n° 1 (à l'attention de la CNRLT) : Au vu du poids des frais bancaires pour les services, engager un dialogue avec la Banque de France tendant à permettre leur réduction.

C. LA LEVÉE D'ANGLES MORTS AU CONTRÔLE DE LA CVFS

**********. Celle-ci étant désormais effective, ce point n'appelle donc plus de remarque.

Les échanges ***** sur le périmètre du contrôle de la commission ont, pour leur part, permis des avancées positives et un contrôle conforme aux prérogatives de la commission. La CVFS considère que tant le périmètre que les modalités du contrôle sont désormais stabilisés.

III. LE SUIVI DES RECOMMANDATIONS DE 2020

● ***Recommandation générale n° 20.01 (à l'attention de la CNRLT) : Au vu de pratiques différentes d'un service à l'autre, s'assurer de la cohérence et du bien-fondé du recours aux fonds spéciaux pour l'acquisition de logiciels.***

Malgré les mesures d'accompagnement mise en place par la CNRLT et la progression du dialogue avec *****, il apparaît qu'une question similaire se pose pour *****.

Cette recommandation reste donc partiellement ouverte.

● ***Recommandation générale n° 20.02 : En lien avec la CNRLT, établir dans chaque service une procédure interne permettant de caractériser l'urgence opérationnelle sur la base d'éléments factuels (date de la demande, délais de procédure, etc.).***

La CVFS prend note du travail mené par la CNRLT pour permettre une définition commune des conditions de l'urgence opérationnelle. Dans l'attente de la concrétisation de ces démarches au sein des services, la recommandation est maintenue.

Cette recommandation reste donc ouverte.

● ***Recommandation générale n° 20.03 (à l'attention de la CNRLT) : Constituer un groupe de travail interservices*** *****

La CVFS constate que malgré la constitution du groupe de travail et la recherche de solutions internes aux différents services, la plupart d'entre eux reste confrontée *****.

Demeurent plusieurs cas de figure :

– la mention sur certaines pièces comptables de l'adresse du service, faute de capacité à pouvoir créer des structures et adresses fictives ;

– la difficulté rencontrée par plusieurs services (DGSI, DRM, DGSE) pour anonymiser les filières d'acquisition de matériels réglementés dès lors qu'un « certificat d'utilisateur final » est signé, ou qu'une déclaration est faite auprès de la « commission R226 » ou de la commission nationale de l'informatique et des libertés (CNIL).

La CVFS constate cependant que *****.

La CVFS réitère son souhait que la question ***** fasse l'objet d'une réflexion conduite par la coordination nationale, et qu'une solution soit prochainement trouvée, sans quoi la commission se verrait contrainte de solliciter la bascule des dépenses correspondantes en fonds normaux.

Cette recommandation reste donc ouverte.

● ***Recommandation générale n° 20.04 : Mettre en œuvre, dans chaque service, un inventaire des matériels acquis en fonds spéciaux,*** *****

La mise en place systématique d'un inventaire des matériels acquis en fonds propres, depuis leur acquisition jusqu'à leur éventuelle cession ou destruction, a été largement mise en œuvre par les services, permettant prochainement un suivi de l'ensemble de ces matériels. *****, la CVFS espère pouvoir rapidement clore cette recommandation.

Cette recommandation reste donc partiellement ouverte.

● ***Recommandation générale n° 20.05 : Accompagner le processus en cours de basculement de fonds spéciaux vers les fonds normaux d'une revalorisation à due proportion des crédits budgétaires alloués aux services et structures concernés.***

La nécessité de poursuivre le déport de certaines dépenses vers les fonds normaux est le pendant de l'augmentation du recours aux fonds spéciaux. La CVFS prend acte de la prise en compte de ce sujet par la CNRLT. La commission constate que de nouvelles dépenses doivent être examinées, *****.

Dans ce contexte, la CVFS reconduit sa recommandation tendant à ce que le basculement vers les crédits généraux s'accompagne d'une revalorisation à due proportion des crédits budgétaires alloués aux services et structures concernés. Un chiffrage devrait être réalisé sous l'égide de la coordination, avant qu'elle n'engage un dialogue sur le sujet avec les services de Matignon.

Cette recommandation reste donc ouverte.

● ***<u>Recommandation générale n° 20.06 (à l'attention de la CNRLT)</u> : Harmoniser les pratiques et les périmètres comptables afin de pouvoir disposer de données consolidées et comparables d'un exercice à l'autre et fournir à la CVFS les raisons des écarts constatés.***

Au regard de l'important travail de consolidation des données mené en 2021, la CVFS clôt cette recommandation.

Cette recommandation est close.

RECOMMANDATIONS GÉNÉRALES 2016, 2017, 2018 ET 2019 RESTANT OUVERTES

N°	Objet	Observations de la CVFS
16.02	Exclusion des fonds spéciaux de l'assiette de calcul de la réserve de précaution du programme 129.	La CVFS se félicite que la réserve de précaution du programme 129 ait systématiquement été levée s'agissant de l'enveloppe de fonds spéciaux, même si elle n'est pas explicitement exclue de l'assiette de calcul de la réserve. Cette recommandation étant prise en compte *de facto*, elle n'a pas lieu d'être reconduite.
16.05	*****	La CVFS se félicite de la progression des travaux menés sur cette question au sein du groupe de travail sur les fonds spéciaux, et suivra leur conclusion avec attention. La CVFS maintient donc sa recommandation.
16.07	Constituer un groupe de travail sur les possibilités de démarquage existantes *****.	La CVFS note que le sujet doit être abordé au sein du « GT Fonds spéciaux ». Dans l'attention des conclusions du groupe de travail, la CVFS maintient sa recommandation.
16.09	Augmenter la dotation en fonds normaux à due proportion des montants transférés en fonds spéciaux.	La CVFS note que le dialogue doit être engagé avec les services de la Première ministre et suivra l'évolution de cette question particulièrement importante. En attendant, la recommandation est reconduite.

N°	Objet	Observations de la CVFS
17.03	Définir des principes et des outils communs à l'ensemble des services spécialisés de renseignement s'agissant du contrôle interne *****: turn-over régulier des agents, élaboration d'indicateurs au niveau central, séparation des fonctions de gestion et de contrôle, *etc.*	La CVFS prend acte des échanges organisés par la CNRLT. Elle constate cependant que des progrès restent à accomplir au sein des services. En conséquence, la commission maintient sa recommandation.
17.04	Encourager la mise en place d'un travail interservices pour définir un cadre de mutualisation *****	La CVFS note avec intérêt les pistes évoquées par la « GT Fonds spéciaux », qui doivent être poursuivies. La CVFS maintient en conséquence sa recommandation et demande à ce que lui soient fournies les futures conclusions du groupe de travail *****.
17.05	*****	Il a été indiqué à la CVFS qu'un groupe de travail permet *****. Tout en admettant que cette solution peut être tout aussi efficace qu'une mutualisation, la commission maintient la recommandation ouverte ; *****.
18.01	Effectuer un « resoclage » de la dotation en fonds spéciaux inscrites au programme 129 pour tenir compte des besoins réels et de l'évolution de l'activité opérationnelle des services.	La CVFS salue l'effort de « resoclage » entrepris par les services du Premier ministre en 2020 et 2021. Elle clôt donc cette recommandation.
18.02	*****.	*****. La commission ***** clôt cette recommandation.
18.04	Désigner par arrêté ou une circulaire, non publié au Journal officiel, les entités et services susceptibles de bénéficier de fonds spéciaux. Cet arrêté ou circulaire, et les modifications apportées ultérieurement, seraient communiqués sans délai à la CVFS.	La CVFS prend note de la proposition de la CNRLT de lui communiquer annuellement la liste des services bénéficiaires de fonds spéciaux. Toutefois, cette communication ne revêt pas le caractère officiel que la commission voulait lui donner, en ce qu'elle formaliserait l'accord de la Première ministre d'attribuer des fonds spéciaux à un nouvel allocataire. En conséquence, la recommandation est reconduite.

N°	Objet	Observations de la CVFS
18.05	Réaffirmer la possibilité pour la CVFS d'accéder aux rapports d'inspection et d'audit interne nécessaires à sa pleine information et à l'exercice de son contrôle, par la diffusion d'une instruction aux services.	La CVFS clôt cette recommandation.
18.06	Mettre en place, au sein de chaque service, un suivi *****.	La commission maintient cette recommandation car aucune information ne lui a été communiquée en ce domaine. Afin de préciser sa demande, elle reformule la recommandation.
18.07	Mettre en place une cellule interservices *****.	La CVFS prend acte de l'existence de ce groupe et renvoie à sa recommandation n° 17.05 *****. En matière *****, elle renvoie à ses recommandations n° 20.01 et n° 20.03. La CVFS clôt donc cette recommandation.
19.02	Remettre à plat, en collaboration avec les services bénéficiaires, les modalités de consolidation des données comptables et budgétaires relatives aux fonds spéciaux et fiabiliser les informations transmises à la CVFS concernant le montant des ressources et des dépenses annuelles, ainsi que le niveau global de la trésorerie en fin d'année.	Au regard des progrès accomplis, la CVFS clôt cette recommandation.
19.03	*****, consulter l'ensemble des services utilisateurs de fonds spéciaux sur leur souhait *****.	La CVFS prend note du fait que ce sujet sera abordé au sein du « GT Fonds spéciaux » au début de l'année 2023. Dans l'attente de la consultation de l'ensemble des bénéficiaires de fonds spéciaux, *****, la recommandation est maintenue.

N°	Objet	Observations de la CVFS
19.04	Mettre en place un groupe de travail transversal à l'ensemble des services bénéficiaires de fonds spéciaux sur les possibilités de discrétion et/ou d'urgence offertes par le droit de la commande publique.	La CVFS prend note du fait que ce sujet sera abordé au sein du « GT Fonds spéciaux » en fin d'année 2022. À l'évidence, certains services n'ont pas connaissance du panel de possibilités qui existent en la matière *****. En attendant la tenue de cette réunion, et des résultats concrets au sein de certains services, la recommandation est maintenue.

*

* *

RECOMMANDATIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT AU TITRE DE SON RAPPORT ANNUEL D'ACTIVITÉ 2022-2023

DOCUMENTS TRANSMIS À LA DÉLÉGATION

Recommandation n° 1 :

Préciser, dans la liste des rapports d'inspection transmise semestriellement à la Délégation parlementaire au renseignement, les services dont émanent lesdits rapports et leur date de publication.

Recommandation n° 2 :

Apporter une réponse dans le délai maximal d'un mois aux demandes de transmission de documents de la Délégation parlementaire au renseignement, formulées au titre de l'article 6 *nonies* de l'ordonnance du 17 novembre 1958.

Recommandation n° 3 :

Engager avec la CNRLT une réflexion sur les modalités de diffusion des rapports classifiés de la Délégation parlementaire au renseignement et de la Commission de vérification des fonds spéciaux.

CELLULE DE RENSEIGNEMENT FISCAL

Recommandation n° 4 :

Associer la Délégation parlementaire au renseignement aux travaux de préfiguration liés à la création de la cellule de renseignement fiscal annoncée le 9 mai 2023 par le Ministre des comptes publics.

INGÉRENCES ÉTRANGÈRES

Recommandation n° 5 :

Organiser dans chaque département, à l'initiative du Préfet et en lien avec les services territoriaux de sécurité intérieure, une session de sensibilisation des élus locaux aux risques d'ingérences après chaque renouvellement électoral (municipal, départemental et régional).

Recommandation n° 6 :

Pérenniser à 10 % (au lieu de 25 %) le seuil de déclenchement de la procédure de contrôle des Investissements Étrangers en France (IEF) non européens.

Recommandation n° 7 :

Présenter chaque année au Parlement, dans le cadre d'un débat sans vote, un rapport sur l'état des menaces qui pèsent sur la sécurité nationale.

Recommandation n° 8 :

S'assurer d'une prise en compte par le PNOR des nouveaux enjeux liés aux ingérences étrangères en rapport avec l'évolution du contexte international et de ses répercussions, notamment en termes d'actions d'influence, d'ingérence et d'espionnage étrangers.

Recommandation n° 9 :

Au vu des enjeux de souveraineté liés à la protection de nos intérêts économiques, engager une réflexion sur un élargissement des missions du Service de l'information stratégique et de la sécurité économique (SISSE) et des moyens humains supplémentaires à lui affecter, en adéquation avec l'état de la menace en matière d'ingérences économiques.

Recommandation n° 10 :

*****

Recommandation n° 11 :

Étendre le dispositif de Protection du potentiel scientifique et technologique de la Nation (PPST) au patrimoine immatériel ainsi qu'à l'ensemble des disciplines universitaires notamment en l'adaptant aux enjeux et influences spécifiques aux sciences humaines et sociales qui en sont exclues.

Recommandation n° 12 :

Inscrire la fonction de fonctionnaire de sécurité et de défense (FSD) dans le référentiel interministériel des métiers de l'État pour la conforter au sein des universités.

Recommandation n° 13 :

Instaurer un dispositif législatif spécifique à la prévention des ingérences étrangères, inspiré du FARA américain ou du futur FIRS britannique.

Recommandation n° 14 :

Étendre, à titre expérimental et pour une durée de 3 ans, le champ d'application de la technique de l'algorithme aux finalités 1 (« indépendance nationale, intégrité du territoire et défense nationale ») et 2 (« intérêts majeurs de la politique étrangère, exécution des engagements européens et internationaux de la France et prévention de toute forme d'ingérence étrangère »).

Recommandation n° 15 :

Élargir le spectre des gels d'avoirs à but antiterroriste (GABAT) à toute personne ou structure se livrant à des actions préjudiciables au maintien de la

cohésion nationale ou destinées à favoriser les intérêts d'une puissance étrangère.

Recommandation n° 16 :

Promouvoir une réponse européenne aux tentatives de déstabilisation liées aux ingérences étrangères autour des orientations suivantes : la mise en place d'instruments juridiques contraignants assortis d'un régime de sanctions, l'amélioration du dispositif européen de cybersécurité *****.

Recommandation n° 17 :

Regrouper dans un projet de loi dédié à la lutte contre les ingérences étrangères les nouveaux dispositifs d'entrave de nature à renforcer notre riposte démocratique.

Recommandation n° 18 :

Orienter le renseignement vers les faiblesses de nos adversaires pour mieux les exploiter dans le débat public.

Recommandation n° 19 :

*****

Recommandation n° 20 :

*****

Recommandation n° 21 :

*****

Recommandation n° 22 :

Augmenter le nombre de coopérants dans les pays d'Afrique australe et de l'océan indien au titre de la politique d'influence de la France.

EXAMEN PAR LA DÉLÉGATION

Réunie le jeudi 29 juin 2023 sous la présidence de M. Sacha Houlié, la Délégation a procédé à l'examen de son rapport annuel.

Après un exposé de son président, la Délégation a adopté son rapport pour 2022-2023 (chapitre I à III), en application du VI de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958.

Par ailleurs, elle avait entendu le 16 février 2023 la présentation du rapport de la Commission de vérification des fonds spéciaux en application du VI de l'article 154 de la loi n° 2001-1275 du 28 décembre 2001 de finances pour 2002 (chapitre IV).

***

SYNTHÈSE DU RAPPORT

CHAPITRE Ier : BILAN D'ACTIVITÉ DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT DE JUILLET 2022 A JUIN 2023

● Le renouvellement de la composition de la DPR au lendemain des élections législatives de juin 2022

La Délégation parlementaire au renseignement a été renouvelée le 28 juillet 2022 pour tenir compte du résultat des élections législatives de juin 2022 et garantir en son sein une représentation pluraliste.

La composition politique de la DPR est la suivante :

Groupe Renaissance : 3 membres (3 députés)
Groupe LR : 3 membres (3 sénateurs)
Groupe SER : 1 membre (sénateur)
Groupe RN : 1 membre (députée)

La DPR est composée de cinq hommes et trois femmes issus des commissions des Affaires étrangères et de la Défense, des Lois et des Finances.

● Une activité soutenue au cours de l'année écoulée

Entre le 1er juillet 2022 et le 30 juin 2023, la DPR a tenu 12 réunions et procédé à l'audition des directeurs des services de renseignement et structures de l'État en lien avec le sujet retenu pour son rapport annuel, à savoir la lutte contre les ingérences étrangères. Le Président de la Délégation a également effectué, du 16 au 22 avril 2023, un déplacement en Afrique du Sud, à l'île de la Réunion et à Madagascar, sur le thème des ingérences étrangères.

La DPR a reçu le 5 octobre 2022 une délégation de députés allemands du Bundestag, membres du PKGr, la commission parlementaire chargée du contrôle de la politique publique du renseignement.

La DPR a également organisé, conjointement avec la Commission nationale de contrôle des techniques de renseignement (CNCTR) un colloque à l'Assemblée nationale, le 11 mai 2023, sur le thème : « ***La politique publique du renseignement est-elle bien contrôlée ?*** ». Ce colloque, dont les actes sont reproduits dans le Tome II du présent rapport, a réuni près de 400 participants issus des services de renseignement, de différents ministères et des diverses autorités de contrôle.

● Les documents transmis à la Délégation

Entre le 1er juillet 2022 et le 30 juin 2023, la DPR a été destinataire d'un certain nombre de documents classifiés parmi lesquels la liste des rapports de l'inspection des services de renseignement et des services d'inspection générale des ministères portant sur les services de renseignement qui relèvent de leur compétence.

La Délégation ou son président a également été destinataire de diverses notes portant notamment sur la technique de l'algorithme ainsi que sur les menaces pour l'ordre public représentées par les groupes liés aux mouvances ultra.

La Délégation a en revanche sollicité la transmission de documents classifiées, mais ses demandes sont restées sans suites. En outre, des documents qui devaient lui être automatiquement transmis au titre de la loi ne l'ont pas été.

La Délégation appelle au respect des dispositions prévues par la loi en matière de communication des documents classifiés, dans le respect de son besoin d'en connaître.

CHAPITRE II :
LES ENJEUX D'ACTUALITÉ LIÉS À LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT

● Le rapport annuel relatif à la politique publique du renseignement (exercice 2021)

Ce chapitre présente les principaux enseignements du rapport annuel relatif à la politique publique du renseignement pour l'exercice 2021, le rapport 2022 n'ayant pas encore été transmis à la Délégation parlementaire au renseignement.

Les faits marquants de l'activité des services en 2021 ont notamment concerné :

*****

Quant aux ressources budgétaires allouées aux service de renseignement – 2,77 milliards d'euros de fonds normaux – elles ont enregistré une légère baisse pour la première fois depuis 2015. En matière de ressources humaines, le total des personnels tous services confondus s'est établi à 20 677 postes en 2021 contre 20 526 en 2020. Le constat le plus notable est celui d'un recours de plus en plus accru à des personnels contractuels (23,69% contre 18,62% en 2017), conjugué à une diminution des recrutements militaires.

● Le volet renseignement de la loi de programmation militaire (LPM) pour les années 2024 à 2030

La loi de programmation militaire pour les années 2024 à 2030 renforce sensiblement les moyens humains et budgétaires alloués aux services de renseignement du ministère des Armées, avec une enveloppe supplémentaire de 5 milliards d'euros sur la période qui va conduire au doublement des budgets de la DGSE, de la DRM et de la DRSD.

La LPM introduit également de nouveaux dispositifs juridiques pour :

– Permettre l'accès des services de renseignement au casier judiciaire au titre des enquêtes administratives de sécurité.

– Permettre la communication par l'autorité judiciaire aux services de renseignement des éléments d'une procédure ouverte pour crime de guerre ou crime contre l'humanité.

– Protéger l'anonymat des anciens agents des services de renseignement ou des anciens membres de forces spéciales dans le cadre des procédures judiciaires.

– Garantir la prise en compte des intérêts fondamentaux de la Nation en cas d'activité privée en rapport avec une puissance étrangère.

● Une nouvelle ambition pour le renseignement fiscal

Le ministre des Comptes publics a annoncé le 9 mai 2023 une série de mesures de lutte contre la fraude fiscale et douanière, parmi lesquelles figure la création envisagée d'une cellule de renseignement fiscal.

Fin 2019, une *task force* opérationnelle dédiée au renseignement fiscal avait été constituée, associant deux services de renseignement du premier cercle (Tracfin et la DNRED) et la direction nationale d'enquêtes fiscales (DNEF).

En annonçant la création d'une cellule dédiée au renseignement fiscal, le Gouvernement souhaite franchir une nouvelle étape et se donner des moyens adaptés pour lutter contre les grands schémas d'évasion et d'opacification fiscales.

Il est envisagé de confier le portage de cette cellule à la DNRED et d'y associer Tacfin, pour ce qui relève de son champ de compétence.

La Délégation parlementaire au renseignement aurait a priori privilégié un portage par Tracfin et souhaite en tout état de cause être associée aux travaux de préfiguration liés à la création de cette cellule de renseignement, au titre de sa mission de « *suivi des enjeux d'actualité et des défis à venir qui s'y rapportent* » inscrite dans la loi.

CHAPITRE III :
LE RENSEIGNEMENT, CŒUR BATTANT DE LA RIPOSTE DÉMOCRATIQUE

AUX INGÉRENCES ÉTRANGÈRES

L'ingérence renvoie à une action dissimulée et malveillante. Commanditée depuis l'étranger, elle vise à porter atteinte, autrement que par la confrontation militaire, à nos intérêts fondamentaux et à notre souveraineté dans toutes ses dimensions politique, juridique, militaire, économique et technologique.

● Les ingérences étrangères en France : une menace protéiforme, omniprésente et qui s'inscrit dans la durée

Bien qu'elle ait toujours existé, la menace liée aux ingérences étrangères est devenue protéiforme, omniprésente et durable. Elle a pris ces dernières années une toute autre dimension sous le triple effet d'une rupture géopolitique majeure – avec le basculement d'un monde de coopération vers un monde de confrontation –, d'une révolution technologique et d'une porosité grandissante entre ce qui relève des affaires intérieures et extérieures, des jeux d'acteurs publics et privés, du global et du local.

Il existe **différentes formes d'ingérences étrangères** : des formes classiques qui relèvent de l'espionnage, des formes modernes dans l'espace cyber et des formes hybrides à travers de vastes opérations de manipulation de l'information et de déstabilisation des processus démocratiques. La Russie et la Chine sont les puissances étrangères les plus impliquées dans les opérations d'ingérence avec des modes opératoires caractéristiques.

La Russie, dans la tradition soviétique, a recours à l'infiltration et à l'espionnage ; le déclenchement de la guerre en Ukraine a conduit à l'expulsion de France de 41 espions russes sous couverture diplomatique. Les opérations de propagande et de manipulation de l'information, couplées à des ingérences fréquentes dans les processus électoraux, sont également caractéristiques de la « signature » russe.

S'agissant de la Chine, la stratégie du « front uni » vise à neutraliser toutes les formes d'opposition au parti communiste chinois, à l'intérieur comme à l'extérieur du pays. La loi chinoise du 28 juin 2017 sur le renseignement national a considérablement étendu les pouvoirs des services de renseignement et fait de tout ressortissant chinois, dans son pays comme à l'étranger, un espion potentiel. La Chine utilise différents leviers d'action pour mener ses opérations d'ingérence : le recours aux diasporas, l'utilisation des médias, la captation de données économiques et scientifiques, la prédation économique.

Au-delà de la Russie et de la Chine, d'autres puissances étrangères ont recours à des actions d'ingérence qu'il s'agisse par exemple de la Turquie à travers le levier de la pratique religieuse, mais aussi de l'Iran et d'autres États du Maghreb et du Golfe. En matière d'espionnage et d'ingérences économiques, nos alliés ne sont pas non plus forcément nos amis et divers modes opératoires, comme l'extraterritorialité du droit, sont utilisés en particulier par les États-Unis

d'Amérique pour capter de la donnée et porter atteinte à notre sécurité économique.

La nouvelle dimension prise par les ingérences étrangères révèle des vulnérabilités persistantes, à commencer par notre naïveté, qui est tant celle des élites politiques et administratives que des milieux économiques et académiques. Une prise de conscience est toutefois en train de s'opérer et des actions de sensibilisation sont désormais régulièrement proposées par nos services de renseignement aux publics identifiés comme des cibles potentielles.

Nos valeurs démocratiques sont à la fois notre force et notre faiblesse face à des régimes autocratiques aux méthodes éloignées des nôtres. Il s'agit de nous protéger en développant des outils efficaces pour lutter contre les ingérences étrangères, sans pour autant rompre avec les valeurs de la démocratie et de l'État de droit.

● La nouvelle priorité donnée à la contre-ingérence ouvre un nouveau cycle du renseignement

L'époque nouvelle que nous traversons est synonyme de changement de cycle pour la communauté du renseignement, ou plus précisément de **chevauchement de deux cycles entre celui du contre-terrorisme, qui reste d'actualité, et celui de la contre-ingérence** qui prend une dimension nouvelle.

Depuis le Livre blanc de 2008 sur la défense et la sécurité nationale, plusieurs documents stratégiques ont annoncé ce changement de paradigme pour la communauté du renseignement. La stratégie nationale du renseignement de juillet 2019 évoque la nécessité de protéger notre souveraineté des ingérences étrangères tandis que la Revue nationale stratégique du 9 novembre 2022 établit une feuille de route dans le contexte géopolitique nouveau lié à la guerre en Ukraine.

Le nouveau cycle du renseignement dans lequel nous sommes entrés se traduit par de **nouvelles organisations internes des services de renseignement**, liés à de nouvelles façons de travailler moins verticales et plus transversales : création de « centres de mission » thématiques et géographiques à la DGSE, *****

La priorité donnée au renseignement se traduit dans l'expression budgétaire de la loi de programmation militaire 2024-2030 qui prévoit de consacrer 5 milliards d'euros supplémentaires aux services de renseignement du ministère des Armées, ce qui signifie un doublement des budgets de la DGSE, de la DRM et de la DRSD d'ici à 2030.

La lutte contre les ingérences étrangères repose, selon ses volets, sur la gouvernance propre aux **services de renseignement** dans les domaines du contre-espionnage, de la contre-influence et du renseignement économique.

Des structures partenaires, qui ne sont pas des services de renseignement, interagissent avec la communauté du renseignement pour détecter, suivre et entraver d'éventuelles actions d'ingérence. Le secrétariat général de la défense nationale (SGDN) joue un rôle important à travers deux agences placées sous son autorité : l'ANSSI pour ce qui relève de la lutte contre les cyberattaques et VIGINUM, l'agence récemment créé pour prévenir et caractériser les opérations de manipulation de l'information. En matière de sécurité économique, le Service de l'information stratégique et de la sécurité économique (SISSE), rattaché à Bercy, est chargé de protéger les actifs stratégiques de l'économie française face aux ingérence étrangères. L'activité de ce service n'a cessé de croître au cours de la période récente, avec un doublement du nombre des alertes mensuelles qui sont passées de 30 en 2020 à près de 60 en 2022.

La lutte contre les ingérences étrangères repose également sur **une dimension interministérielle renforcée**, tant au niveau stratégique qu'opérationnel. S'agissant de la protection de nos intérêts économiques, un conseil de sécurité et de défense en format « sécurité économique » existe depuis 2017 sous l'autorité du Président de la République. Un comité interministériel unique (le COLISE), présidé par le SGDSN, contribue à orienter l'action des services de renseignement vers les priorités identifiées. La cyberdéfense s'est également interministérialisée avec la création d'un CODIR Cyber au niveau stratégique et d'un centre de coordination des crises cyber à l'échelon opérationnel. La riposte aux opérations de manipulation de l'information repose pour sa part sur le comité opérationnel de lutte contre les manipulations de l'information (COLMI) placé sous l'autorité du SGDSN.

Les services de renseignement peuvent recourir à **divers moyens d'entrave** pour contrecarrer les ingérences étrangères :

– **Les techniques de renseignement,** au titre de la finalité 2 qui correspond à « *la prévention de toute forme d'ingérence étrangère* ». *****.

– **Les mesures d'ordre diplomatique** avec la procédure de *persona non grata* qui a permis à la France d'expulser 41 espions russes sous couverture diplomatique au lendemain de l'invasion de l'Ukraine.

– **Les mesures pénales** qui permettent de sanctionner des faits avérés d'espionnage au titre du délit d'atteinte aux intérêts fondamentaux de la Nation.

– **Les mesures d'ordre économique** avec le dispositif de contrôle des investissements étrangers en France (IEF) et la loi dite « de blocage » de 1968.

– Le dispositif de **protection du potentiel scientifique et technique de la Nation** (PPST) qui prévoit notamment la création de « zones à régime restrictif » (ZRR) pour limiter l'accès à des lieux hébergeant des données

sensibles.

– Les dispositions de la **loi « séparatisme » du 24 août 2021** confortant le respect des principes de la République qui fixe notamment de nouvelles règles pour le financement étranger des lieux de culte et des écoles privées hors contrat.

Pour autant, **ces outils ne suffisent pas à eux seuls à entraver dans la durée des tentatives d'ingérences de plus en plus nombreuses et protéiformes.** Aussi, la Délégation parlementaire au renseignement estime nécessaire de se doter de moyens d'entrave supplémentaires pour contrecarrer des actions hostiles à nos intérêts fondamentaux. La loi de programmation militaire 2024-2030 prévoit ainsi que le ministre des Armées pourra désormais s'opposer au recrutement par une puissance étrangère d'anciens militaires détenteurs de savoir-faire militaires opérationnels rares.

Parmi les mesures nouvelles proposées par la Délégation parlementaire au renseignement figurent notamment :

– Des mesures de sensibilisation plus systématiques aux risques d'ingérences et la remise chaque année au Parlement d'un **rapport sur l'état des menaces** qui pèsent sur la sécurité nationale. Ce rapport pourrait faire l'objet d'un débat (sans vote) en séance publique.

– L'instauration d'un **dispositif législatif *ad hoc* de prévention des ingérences étrangères,** sur le modèle de la loi américaine (FARA). Il s'agirait de rendre obligatoire l'enregistrement des acteurs influant sur la vie publique française pour le compte d'une puissance étrangère et de les soumettre à une série d'obligations déontologiques.

– L'expérimentation à la lutte contre les ingérences étrangères, de l'utilisation de la **technique de l'algorithme**, aujourd'hui réservée exclusivement à la prévention du terrorisme.

– Le recours à la **procédure des gels d'avoirs** à toute personne ou structure se livrant à des actions préjudiciables au maintien de la cohésion nationale ou destinée à favoriser les intérêts d'une puissance étrangère.

– Une **réponse européenne** fondée notamment sur une convergence des dispositifs nationaux de lutte contre les ingérences étrangères.

Ces différentes mesures pourraient être regroupées dans un **projet de loi dédié à la lutte contre les ingérences étrangères** afin de provoquer un débat public global sur ce sujet.

● Les positions stratégiques françaises à l'épreuve des ingérences étrangères en Afrique australe et dans l'Océan indien

Les ingérences étrangères ne concernent pas que le territoire national ;

elles ciblent également les intérêts français à l'étranger. En Afrique Australe et dans l'océan indien, la France à des intérêts majeurs à défendre et notre appareil de renseignement joue un rôle essentiel pour révéler les stratégies, mesurer les enjeux et préparer l'avenir.

En Afrique, la réalité **d'États faillis** a laissé le champ libre à des puissances étrangères. Mais d'autres facteurs peuvent constituer un terreau favorable aux ingérences, à commencer par l'existence de **liens historiques de certains pays avec des puissances étrangères**. La dette morale de l'Afrique du Sud envers la Russie, très forte au vu de soutien que l'Union soviétique a apporté à la lutte contre l'Apartheid, explique aujourd'hui la proximité qui existe entre les deux pays. Les relations actuelles entre Madagascar et la Russie sont aussi pour le moins complexes. Il est notamment établi que la Russie a tenté d'interférer dans le cours de l'élection présidentielle malgache de 2018.

Les ingérences étrangères sont essentiellement le fait de deux pays, la Russie et la Chine, avec des modes opératoires bien distincts.

En ce qui concerne la Russie, il s'agit de la propagande, de la vente d'armes, de la conclusion d'accords de coopération militaire et d'investissements dans le secteur minier.

S'agissant de la Chine, ce sont des investissements dans les infrastructures et les ressources naturelles, le *soft power* (institut *Confucius*) et la conclusion d'accords de coopération militaire.

La contestation des intérêts français dans cette région du monde s'inscrit dans **une stratégie délibérée de francophobie** et prend des formes multiples telles que des opérations de manipulation de l'information visant à porter atteinte à l'image et à la réputation de la France, procès politiques, actions hostiles aux entreprises françaises et à nos intérêts économiques.

Au-delà des intérêts français, **c'est aussi la souveraineté de la France dans cette région du monde qui est remise en cause**. Notre présence dans l'océan indien constitue 93% de la zone économique exclusive (ZEE) de la France. Certains territoires, habités ou non, font l'objet de contentieux anciens entre la France et plusieurs États que sont notamment Maurice (Tromelin) et Madagascar (îles Eparses). La situation à Mayotte est également un sujet de tension majeur entre la France et les Comores comme l'a illustré l'opération Wuambushu lancée en mai 2023. **Ces contentieux et ces tensions sont régulièrement instrumentalisés par des puissances étrangères** qui les utilisent pour nuire à nos intérêts fondamentaux. La Russie, ne manquent jamais une occasion de rappeler son soutien à la revendication de Madagascar sur les îles Éparses tandis qu'aux Comores, Moscou joue des tensions liées à la situation à Mayotte, allant même jusqu'à se prononcer en faveur d'une « Mayotte comorienne ».

Dans ce contexte, nos services de renseignement sont orientés dans une stratégie de riposte fondée sur **l'exploitation des faiblesses de nos adversaires et le développement de partenariats avec des pays qui ne font pas partie de notre sphère historique d'influence.**

Derrière les apparences, la Russie et la Chine sont loin d'être en terrain conquis dans les pays qu'ils investissent. Tout en accusant l'occident de néocolonialisme, **la Russie et la Chine se comportent en réalité comme des prédateurs**, pillant les ressources naturelles des pays qu'ils exploitent, peu scrupuleux du respect de l'environnement exerçant leur mainmise sur la souveraineté même de ces États.

Ces puissances étrangères ne contribuent en rien à dynamiser l'économie des pays concernés ; au contraire, la violence à l'égard des populations locales est de mise, assortie de racisme et qui s'accompagne d'un sentiment d'abandon des populations locales. *Wagner* subit des échecs, notamment au Mozambique, où la milice paramilitaire a dû reculer au bout de deux mois face au groupe armé État islamique (EI). L'enjeu n'est pas seulement de détecter les faiblesses et de fournir du renseignement, mais bien d'exploiter ce renseignement de façon appropriée et réactive. **Le renseignement devient une arme à part entière pour exploiter au mieux les failles de ceux que l'on combat.**

Parce que la nature a horreur du vide, il est aussi nécessaire de mieux valoriser et d'amplifier l'action de la France dans les pays où nous sommes présents. En d'autres termes, il s'agit de **rendre la marche plus haute pour ceux qui voudraient nuire à nos intérêts.**

Il existe en Afrique Australe un certain nombre de pays qui sont en demande de coopérer davantage avec la France. Il importe ainsi d'identifier les États avec lesquels nous pourrions développer des coopérations en matière de sécurité et de renseignement. *****.

Enfin, même s'il ne s'agit pas de renseignement à proprement parler, il serait judicieux de **repenser notre dispositif de coopération**. Le nombre de coopérants français n'a cessé de diminuer au cours des dernières années, marqueur de la volonté politique de tourner la page de la françafrique. Pour autant, dans le contexte d'intensification des ingérences étrangères, les coopérants sont des relais privilégiés qui contribuent utilement à une stratégie d'influence.

CHAPITRE IV :
RAPPORT GÉNÉRAL DE LA COMMISSION DE VÉRIFICATION DES FONDS SPÉCIAUX (EXERCICE 2021)

Ce chapitre traite des conditions d'emploi des fonds spéciaux au cours de l'exercice 2021. Ceux-ci ont représenté un montant de ***** en 2021, ***** par rapport à 2020 *****. Les dépenses en fonds spéciaux ont représenté *****. Les

observations de la CVFS, communes à l'ensemble des services de renseignement, sont les suivantes :

-La nécessité d'une application stricte de la doctrine d'emploi des fonds spéciaux.
- Le poids parfois disproportionné des frais bancaires supportés par les services.
- La levée d'angles morts au contrôle de la CVFS *****.