N° 2248
ASSEMBLÉE NATIONALE
CONSTITUTION DU 4 OCTOBRE 1958
DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale
le 16 décembre 2025

N° 227
SÉNAT
SESSION ORDINAIRE DE 2025-2026

Enregistré à la Présidence du Sénat
le 16 décembre 2025

RAPPORT PUBLIC

FAIT

AU NOM DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

*relatif à l'***activité** *de la* **délégation parlementaire** *au* **renseignement**
pour l'année **2025**

TOME I

« LA TRANSFORMATION DU RENSEIGNEMENT FRANÇAIS FACE AUX RUPTURES DU MONDE »

Par
M. Jean-Michel JACQUES,
Député

Déposé sur le Bureau de l'Assemblée nationale

par M. Jean-Michel JACQUES,
Président de la délégation

Déposé sur le Bureau du Sénat

par Mme Muriel JOURDA,
Première vice-présidente de la délégation

SOMMAIRE

___

AVANT-PROPOS

Mesdames, Messieurs,

L'année 2025 confirme, avec une acuité particulière, la place désormais centrale occupée par le renseignement pour assurer notre autonomie stratégique et garantir l'exercice effectif de la souveraineté nationale. Dans un environnement géopolitique profondément dégradé, marqué par une conflictualité de haute intensité, la remise en cause des équilibres multilatéraux, la persistance du terrorisme djihadiste et l'affirmation de puissances hostiles à nos valeurs et à nos intérêts, le renseignement constitue plus que jamais un outil décisif de compréhension, d'anticipation et de protection.

Dans ce contexte durablement instable, la feuille de route des services de renseignement répond à une nouvelle doctrine qui repose sur la *Revue nationale stratégique* publiée à l'été 2025 et sur une stratégie nationale du renseignement elle aussi mise à jour. Ces documents de référence traduisent la volonté au plus haut niveau de l'État de doter la communauté du renseignement d'une vision claire et d'un cadre stratégique, juridique et éthique incontestable.

Au terme d'une première décennie de mise en œuvre de la loi « renseignement » de 2015, la politique publique du renseignement prend une dimension nouvelle ; son contrôle aussi.

Alors que la loi confie désormais à la Délégation parlementaire au renseignement « *le suivi des enjeux d'actualité et des défis à venir qui s'y rapportent* », le contrôle parlementaire de la politique publique du renseignement doit servir la légitimité démocratique de l'action des services. Il doit garantir que l'efficacité opérationnelle ne contrevienne pas à l'État de droit alors que le point d'équilibre entre sécurité nationale et protection des libertés publiques est en questionnement permanent, comme l'a souligné la virulence du débat parlementaire sur le chiffrement et l'accès finalement refusé aux messageries cryptées.

Notre délégation est ainsi appelée à exercer un contrôle exigeant et permanent sur une politique publique qui se construit dans le temps long, dans la transparence vis-à-vis du Parlement et dans l'évaluation continue des moyens et des missions. L'articulation des travaux de la DPR avec ceux, en son sein, de la commission de vérification des fonds spéciaux, est à cet égard déterminante pour assurer la plénitude du contrôle parlementaire.

Dans ce monde nouveau où les périls s'agrègent, se répondent et se renforcent, la DPR a décidé de consacrer le thème central de son rapport annuel aux transformations en cours au sein de la communauté du renseignement, appelée à repenser son organisation et ses méthodes de travail pour faire face à la dangerosité du monde et pour détecter et entraver des modes opératoires de plus en plus sophistiqués. Ces enjeux et ces défis ont été abordés lors du colloque consacré au « *renseignement français face au désordre mondial* » qui s'est tenu le 4 décembre 2025 dans la Galerie des Fêtes de l'Assemblée nationale, à l'initiative de la DPR et dont les actes sont publiés dans le tome II du présent rapport.

Au terme de ses travaux, auditions et déplacements menés tout au long de l'année 2025, la délégation parlementaire au renseignement veut partager cette conviction que le renseignement n'est pas une politique publique périphérique ou strictement spécialisée, mais bien l'un des piliers de la sécurité nationale, de la résilience et de la capacité de la France à continuer à peser dans les affaires du monde, sans jamais se renier, fidèle à elle-même, à ses valeurs et au respect du droit et de la démocratie.

___

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 :
ACTIVITÉ DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT AU COURS DE L'ANNÉE 2025

I. LA COMPOSITION DE LA DÉLÉGATION

Conformément à l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958, les présidents des commissions chargées des affaires de sécurité et de défense des deux chambres sont membres de droit de la Délégation. La Présidence de la délégation est assurée, alternativement, pour un an, par un député ou un sénateur membre de droit.

Lors de sa réunion du 17 décembre 2024, la délégation parlementaire au renseignement a procédé à l'élection de son nouveau président pour l'année 2025. Elle a également procédé à l'élection d'un nouveau Bureau.

La composition de la Délégation fut la suivante en 2025 :

– M. Jean-Michel Jacques, député (EPR) du Morbihan, Président, membre de droit.

– Mme Muriel Jourda, sénatrice (LR) du Morbihan, première vice-présidente, membre de droit.

– M. Aurélien Rousseau, député (app. SOC) des Yvelines, vice-président.

– M. Florent Boudié, député (EPR) de la Gironde, membre de droit.

– M. Cédric Perrin, sénateur (LR) du Territoire de Belfort, membre de droit.

– Mme Catherine Di Folco, sénateur (LR) du Rhône (jusqu'en mars 2025) puis Mme Agnès Canayer, sénateur (LR) de la Seine-Maritime depuis mars 2025.

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

– Mme Gisèle Jourda, sénatrice (SER) de l'Aude.

La loi fixe l'exigence d'une représentation politique pluraliste au sein de la délégation parlementaire au renseignement, en tenant compte de la composition de chaque chambre du Parlement. Quatre groupes politiques sont ainsi représentés reflétant des équilibres politiques différents entre l'Assemblée nationale et le Sénat.

Composée d'autant de femmes que d'hommes, la Délégation satisfait parfaitement au principe de parité.

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

La Délégation parlementaire au renseignement s'est réunie mensuellement au cours de l'année 2025. Dans le cadre de sa mission de contrôle et d'évaluation de la politique publique du renseignement, elle a auditionné les personnes suivantes :

– Jeudi 23 janvier 2025 :

- **Mme Céline Berthon**, directrice générale de la sécurité intérieure (DGSI).
- **M. Sébastien Tiran**, directeur de la direction nationale du renseignement douanier (DNRED).

– Jeudi 13 février 2025 :

- **GCA Jacques Langlade de Montgros**, directeur du renseignement militaire (DRM).

– Jeudi 20 mars 2025 :

- **M. Pascal Mailhos**, coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT).
- **M. Antoine Magnant**, directeur de Tracfin.

– Jeudi 10 avril 2025 :

- **Mme Camille Hennetier**, cheffe du service national du renseignement pénitentiaire.
- **M. Hugues Bricq**, directeur du renseignement de la Préfecture de Police de Paris.

– Jeudi 22 mai 2025 :

- **M. Nicolas Lerner**, directeur général de la sécurité extérieure (DGSE).

– Jeudi 26 juin 2025 :

- **M. Vincent Mazauric**, président de la Commission nationale de contrôle des techniques de renseignement (CNCTR).
- **M. Nicolas Roche**, secrétaire général de la défense et de la sécurité nationale (SGDSN).

– Jeudi 25 septembre 2025 :

- **M. Jean Maïa**, président de la Haute autorité pour la transparence de la vie publique (HATVP).

La Délégation a par ailleurs effectué **un déplacement en Pologne et en Lettonie** du 12 au 14 novembre 2025, commun avec la Commission de vérification des fonds spéciaux, auquel ont participé Mmes Agnès Canayer, Caroline Colombier et Gisèle Jourda.

La commission de vérification des fonds spéciaux a aussi effectué, du 25 au 28 mars 2025, un déplacement à l'étranger *****. Elle s'est également rendue à Marseille les 21 et 22 octobre 2025 auprès des directions zonales de la DGSI, de la DNRED et de la cellule interrégionale du renseignement pénitentiaire.

Ces contrôles sur place et sur pièces de la CVFS, participent pleinement à la mission de contrôle parlementaire qui incombe à la DPR, en ce qu'ils permettent d'évaluer comment se met en œuvre, sur le terrain, la politique publique du renseignement. La DPR et la CVFS sont clairement les deux faces d'un seul et même contrôle.

Une présentation du contrôle parlementaire de la politique publique du renseignement a également été organisée le 8 octobre 2025 pour les auditeurs du cycle des hautes études de l'Académie du renseignement.

Enfin, la Délégation a organisé, le 4 décembre 2025 à l'Assemblée nationale (Galerie des fêtes) **un colloque sur le thème : « Le renseignement français face au désordre mondial »** qui a réuni environ 400 personnes. Les actes de ce colloque font l'objet d'une publication dans le tome II du présent rapport.

III. LES DOCUMENTS TRANSMIS À LA DÉLÉGATION

Plusieurs documents classifiés ont été transmis au Président de la Délégation au cours de l'année 2025 :

_ *****

– En application de la loi, la délégation est chaque année destinataire 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, ainsi que du rapport annuel de synthèse exhaustif des crédits consacrés au renseignement. Ces documents lui ont été remis tardivement, le 27 novembre 2025, alors que la CNRLT, par une note en date du 6 mars 2025, avait pris l'engagement de diffuser ce rapport à compter du 31 juillet 2025.

– Le 6 octobre 2025 a été communiquée, par la CNRLT, au président de la Commission de vérification des fonds spéciaux (CVFS) la note annuelle sur la gestion des fonds spéciaux et le suivi des recommandations de la CVFS.

– À sa demande, la délégation a obtenu la communication, en septembre 2025, de la version classifiée de l'objectif stratégique n° 8 (« une autonomie d'appréciation et une souveraineté décisionnelle garanties ») de la *Revue nationale stratégique*.

– Enfin, en application de l'article 6 *nonies* 7° de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, la liste des rapports réalisés par l'inspection des services de renseignement (ISR) est communiquée à la Délégation parlementaire au renseignement. La CNRLT a indiqué le 11 décembre 2025 à la DPR qu'en 2025, l'ISR avait réalisé un seul rapport, dédié à l'évaluation du projet de renforcement de la sous-direction de l'anticipation opérationnelle de la direction générale de la gendarmerie nationale.

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

RAPPORT 2023-2024

Complètement prise en compte	8	13
En cours de prise en compte	5	
Non prise en compte	4	
Non cotée	11	
TOTAL	**28**	

B. LE SUIVI DES RECOMMANDATIONS DES RAPPORTS ANTÉRIEURS

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**	

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 DU RAPPORT ANNUEL RELATIF À LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT (EXERCICE 2024)

La Délégation parlementaire au renseignement (DPR) a été destinataire, début décembre 2025, 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, pour l'exercice 2024. Ce rapport lui a été transmis par M. le préfet Pascal Mailhos, coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT).

A. UNE ANNÉE MARQUÉE PAR LES JEUX OLYMPIQUES ET PAR LA LUTTE CONTRE LES INGÉRENCES ÉTRANGÈRES

1. Les Jeux Olympiques et Paralympiques de 2024

Le rapport transmis par le CNRLT fait un point tout d'abord sur les dispositifs mis en place à l'occasion des Jeux olympiques et paralympiques (JOP) de 2024, avec notamment la création d'un Centre du renseignement olympique (CRO), positionné au sein de la Coordination nationale pour la sécurité des jeux olympiques (CNSJ) et du Centre national de commandement stratégique (CNCS). Le rôle du CRO, déjà testé avec succès lors de la coupe du monde de rugby de 2023, a été jugé très positivement.

Une mission d'évaluation de la préparation des services de renseignement aux JOP 2024 avait par ailleurs été confiée à l'Inspection des services de renseignement (ISR) au printemps 2023. Les recommandations de l'ISR ont été mises en œuvre de manière très satisfaisante à l'automne suivant.

Le rapport d'activité souligne aussi le succès de la stratégie d'entraves judiciaire et administrative à l'encontre des objectifs violents, portée notamment par la circulaire du ministre de l'Intérieur du 6 mai 2024, même si la médiatisation de celle-ci a permis à certains objectifs d'adapter leur comportement (fuite, modifications, dissimulations, etc.).

En termes de bilan, mis à part les actes et tentatives de sabotages à l'encontre des réseaux ferrés et de communications, les JOP ne se sont pas heurtés à des problèmes significatifs de sécurité, en dépit des multiples menaces identifiées (terroriste, ordre public, criminelle, informationnelle, etc.). ***** La menace cyber enfin s'est au final révélée plus faible qu'anticipée.

2. L’adoption de la loi visant à prévenir les ingérences étrangères

Un autre fait marquant de l’année 2024 a été l’adoption de la loi n° 2024-850 du 25 juillet visant à prévenir les ingérences étrangères, issue d’une proposition de loi déposée par le député Sacha Houlié. Plusieurs besoins législatifs étaient en effet apparus depuis l’adoption de la loi du 30 juillet 2021 relative à la prévention d’actes de terrorisme et au renseignement.

Le texte adopté s’appuie sur les conclusions du rapport de la DPR de l’année 2023. Il s’inspire aussi de la loi américaine dite « FARA » (*Foreign Agents Registration Act*) relative à l’enregistrement des agents étrangers ainsi que de la loi britannique de 2023 sur la sécurité nationale instaurant un registre portant sur les influences étrangères (*Foreign Influence Registration Scheme* ou FIRS). La loi du 25 juillet 2024 crée un répertoire, confié à la Haute autorité pour la transparence de la vie publique (HATVP), recensant les représentants d’intérêts exerçant des activités d’influence pour le compte d’un mandant étranger. Les think-tanks recevant des financements de puissances ou d’entités étrangères sont par ailleurs tenus de déclarer ceux-ci à la HATVP. La loi étend, à titre expérimental, l’usage par les services de renseignement de la technique de l’algorithme (traitements automatisés de données) aux cas d’ingérences étrangères (et plus seulement à la seule fin de prévention du terrorisme). Elle crée un nouvel article 411-12 du Code pénal qui érige en circonstance aggravante le fait de commettre certains crimes ou délits dans le but de servir les intérêts d’une puissance ou d’une entité étrangère. La loi de 2024 permet enfin de geler les avoirs des personnes physiques ou morales pratiquant des actes d’ingérences étrangères.

B. DES MOYENS ET UNE ACTIVITÉ EN HAUSSE, SOUS LE CONTRÔLE DE DIVERS ORGANES

1. L’activité des services en 2024

Le rapport 2024 transmis par le CNRLT dresse un bilan de l’activité des services de renseignement au cours de l’année écoulée. Comme le souligne le rapport, cette activité peut être rattachée à trois types d’objectifs : l’aide à la décision, la prévention et la réduction des vulnérabilités et enfin l’entrave et la neutralisation des menaces.

En matière d’aide à la décision (rédaction de divers types de notes), l’activité des services spécialisés s’est répartie de façon homogène. *****.

S’agissant de l’activité des services spécialisés en matière de prévention et de réduction des vulnérabilités, elle est nette progression en 2024, comme l’année passée, en raison notamment de la forte hausse des enquêtes administratives élémentaires sur personne physique menées par la DGSI. *****.

En ce qui concerne enfin l'entrave et la neutralisation des menaces, cette activité s'inscrit à plus de 90 % dans l'axe de la lutte contre la menace terroriste.

Le nombre d'actions menées par les services spécialisés de renseignement a plus que doublé entre 2023 et 2024. Ceci s'explique notamment par la multiplication par plus de quatre du nombre de propositions d'interdiction administrative du territoire, dans le contexte en particulier d'une hausse des sorties de détention des détenus TIS (terrorisme islamiste sunnite) ou RAD (radicalisés).

Dans le rapport d'activité 2024 de la CNCTR, auquel se réfère le rapport transmis par le CNRLT, il est fait état d'une stabilisation globale des personnes surveillées (24 308 en 2024 contre 24 209 en 2023), malgré un niveau très élevé de menaces en 2024 (situation internationale, événements sportifs, violences collectives en Nouvelle-Calédonie, *****). La prévention du terrorisme est redevenue en 2024 la première finalité en nombre tant de personnes surveillées que de techniques mises en œuvre. Le nombre de personnes surveillées au titre de la prévention des extrémismes violents poursuit en revanche sa baisse. La CNCTR relève par ailleurs une forte hausse du nombre de demandes concernant la technique du recueil de données informatiques (RDI) en vue de pallier les difficultés liées à l'usage des canaux chiffrés de communication.

Le rapport d'activité 2024 communiqué par le CNRLT précise que, s'agissant des techniques de renseignement soumises à autorisation sur le territoire national, le nombre de demandes a augmenté de près de 4,2 % en 2024. *****.

Parmi les sept finalités possibles pouvant justifier le recours à une TRR (technique de recueil de renseignement) soumise à autorisation, la prédominance de la finalité 4 (prévention du terrorisme) est confirmée puisqu'elle représente 39 % des demandes en 2024, tous services confondus. *****.

2. Les moyens des services en 2024

Pas moins de 14 programmes budgétaires concourent à la politique publique du renseignement. Pour 2024, l'enveloppe globale des crédits de paiement en fonds normaux s'est établie à 3,4 milliards d'euros, soit une hausse de 10,26 % par rapport à l'exercice précédent.

****

S'agissant des fonds spéciaux, leur montant a augmenté, de 2020 à 2024, *****. La dotation initiale pour 2024 était en baisse ***** en début d'exercice. *****. La Commission de vérification des fonds spéciaux soulève néanmoins un problème de sincérité budgétaire *****.

En matière de ressources humaines, les effectifs des services spécialisés ont poursuivi leur progression, atteignant 16 150 agents en 2024, contre 15 816 en 2023. Ils étaient de 14 912 en 2020. Cette hausse est portée par celle des effectifs de la DGSE ***** et de la DGSI *****. Pour ces deux services, la hausse des

effectifs est respectivement de 9,08 % et de 10,72 % entre 2020 et 2024. S'agissant des services mentionnés à l'article L. 811-4 du code de la sécurité intérieure, leurs effectifs globaux tendent à se stabiliser, passant de 4 170 en 2023 à 4 177 en 2024.

3. Les contrôles exercés en 2024 sur la politique du renseignement

En plus des contrôles internes aux services et de ceux de la DPR et de la CVFS, la politique du renseignement a fait l'objet en 2024 de multiples contrôles externes. La Cour des comptes a ainsi produit un rapport sur la DNRED dont la validation est intervenue en novembre ainsi qu'un rapport dédié au SNRP dont la version définitive a été diffusée en juin. La juridiction financière a également entamé un contrôle sur la gestion des ressources humaines dans les services de renseignement. De son côté, l'Inspection des services de renseignement (ISR) a achevé en 2024 une mission sur le renseignement d'origine sources ouvertes. La CNCTR, pour sa part, a effectué de multiples contrôles tant *a priori* qu'*a posteriori.*

II. LA LOI N° 2025-532 DU 13 JUIN 2025 VISANT À SORTIR LA FRANCE DU PIÈGE DU NARCOTRAFIC

A. UNE LOI QUI SIMPLIFIE LES PROCÉDURES APPLICABLES AUX SERVICES DE RENSEIGNEMENT ET AMÉLIORE LES MODALITÉS DE PARTAGE D'INFORMATIONS

Issue d'une proposition de loi des sénateurs MM. Étienne Blanc et Jérôme Durain, la loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic – tout comme la loi organique relative au statut du procureur de la République anticriminalité organisée, qui procède de la même réforme – a été définitivement adoptée le 29 avril 2025.

Elle s'appuie sur les conclusions d'une commission d'enquête du Sénat [(1)], qui soulignait la nécessité d'« *assumer l'importance du renseignement administratif pour la lutte contre le narcotrafic* » et appelait à approfondir deux chantiers complémentaires « *[l'un] sur la place du renseignement dans la lutte contre ce phénomène, l'autre sur l'articulation entre le renseignement et le judiciaire* ».

Concernant ce second axe, l'article 13 de la loi étend le dispositif de transmission d'informations entre les juridictions et les services de renseignement, en vue de permettre la communication aux services de renseignement d'éléments utiles qui n'ont pas été exploités en procédure. Répliquant les dispositions applicables en matière de terrorisme, cette mesure élargit en conséquence la dérogation au secret de l'enquête et de l'instruction pour les faits relevant de la criminalité et de la délinquance organisées.

(1) Rapport n° 588 (2023-2024), « Un nécessaire sursaut : sortir du piège du narcotrafic *», déposé le 7 mai 2024*

À l'initiative des sénateurs membres de la DPR, le périmètre organique et matériel du dispositif a été circonscrit. La faculté de communication d'informations a été recentrée sur le seul Parquet national anticriminalité organisée (PNACO) et sur les juridictions interrégionales spécialisées (JIRS), excluant ainsi les procureurs de droit commun. Le champ des infractions susceptibles de donner lieu à transmission a également été resserré.

S'agissant du premier axe, relatif à la reconnaissance du rôle structurant du renseignement administratif dans la lutte contre les trafics et à la nécessité d'une meilleure réactivité opérationnelle, le législateur a simplifié certaines procédures applicables. Dans ce cadre, afin de fluidifier la coopération interservices, et sur proposition des sénateurs membres de la DPR, l'article 1er assouplit les conditions de transmission d'informations entre les services du « premier cercle » et l'ensemble des services dits « du second cercle » (police et gendarmerie nationales, préfecture de police, administration pénitentiaire). L'autorisation du Premier ministre, après avis de la CNCTR, n'est ainsi désormais plus requise lorsque des renseignements sont transmis à des services du « second cercle » pour une finalité distincte de celle ayant justifié leur recueil.

Dans le même esprit, l'article 17 aligne la durée autorisée pour pénétrer dans un lieu privé en vue d'installer une technique de renseignement sur la durée de mise en œuvre de cette même technique. Cette mise en cohérence, conforme à une recommandation formulée par la CNCTR dans son rapport d'activité pour 2023, entraîne un doublement de la durée d'autorisation pour la pose des dispositifs techniques.

Le texte a par ailleurs servi de véhicule législatif pour intégrer des mesures propres au renseignement. Ainsi, l'article 16 proroge jusqu'au 31 décembre 2028 l'expérimentation des interceptions de communications satellitaires. Autorisée par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, cette technique peut être mobilisée lorsque les interceptions classiques auprès des opérateurs de communication ne sont pas envisageables. Elle permet aux services de renseignement d'intercepter directement, au moyen d'un dispositif de captation spécifique, les correspondances émises ou reçues par voie satellitaire, sans recourir à l'intervention des opérateurs. *****.

B. UN EXAMEN PARLEMENTAIRE QUI RÉVÈLE DES ENJEUX EN SUSPENS LIÉS AUX NOUVELLES TECHNIQUES DE RENSEIGNEMENT

Les travaux parlementaires ont mis en lumière les enjeux spécifiques liés à l'essor de nouvelles techniques de renseignement, dont la sophistication technologique et le degré d'intrusivité conduisent à reconsidérer l'équilibre entre les impératifs de sécurité publique et la protection des libertés fondamentales – en particulier le respect de la vie privée et la protection des données personnelles – et confèrent, de ce fait, un rôle renouvelé au Parlement dans la conciliation de ces exigences et l'appréhension technique des usages.

Deux dispositifs ont fait l'objet d'une attention particulière : d'une part, les conditions d'accès aux messageries cryptées, et d'autre part, les techniques de renseignement algorithmique, sur lesquelles le Conseil constitutionnel a été amené à se prononcer.

1. L'accès aux messageries cryptées

Introduit au Sénat par un amendement de M. Cédric Perrin [(1)], après avis défavorable de la commission et avis favorable du gouvernement, l'article 8 *ter* de la proposition de loi entendait redéfinir les obligations des opérateurs et fournisseurs de services en ligne dans le cadre des réquisitions. Il proposait de remplacer l'obligation de fournir des données chiffrées accompagnées de leurs clés de déchiffrement par une obligation de transmettre directement des données intelligibles, sans que puissent être invoquées des contraintes liées à l'architecture technique des systèmes. Cette problématique a été soulevée par le CNRLT et rappelée par le ministre de l'Intérieur.

L'intention poursuivie était de répondre au défi posé par la généralisation du chiffrement « de bout en bout », qui garantit que seules les parties à une communication peuvent en déchiffrer le contenu mais qui réduit, en conséquence, l'efficacité des mécanismes actuels de réquisition des données à l'encontre des personnes faisant l'objet d'une enquête administrative des services.

Supprimé en commission à l'Assemblée nationale, l'article n'a pas été rétabli en commission mixte paritaire.

Au-delà des interrogations sur la proportionnalité du dispositif, ce sont surtout les contraintes techniques et les risques de cybersécurité – recours à de prétendues « portes dérobées », car tel n'était pas l'objet de l'amendement, ou à des « clés de déchiffrement maîtresses » – qui ont conduit l'Assemblée nationale puis, *in fine*, le Parlement à surseoir. L'introduction de ce dispositif par amendement, sans étude d'impact, n'a en effet pas permis d'évaluer de manière satisfaisante la faisabilité et les conséquences du mécanisme proposé.

Ces interrogations ont trouvé un nouvel écho lors de l'examen, en mars 2025, du projet de loi relatif à la résilience des infrastructures critiques et à la cybersécurité. En réaction aux débats suscités par l'examen de la loi « narcotrafic », le Sénat a adopté un article 16 *bis* interdisant d'imposer aux opérateurs l'intégration de portes dérobées, de clés maîtresses ou de tout mécanisme conduisant à un affaiblissement volontaire de la sécurité de systèmes. Selon l'auteur de

(1) Amendement n° 73 rectifié ter, déposé par M. Cédric Perrin, instaurant pour les plateformes une obligation de mettre en œuvre des mesures techniques pour l'accès au contenu intelligible des correspondances et données ayant fait l'objet d'une autorisation spécifique de mise en œuvre des techniques de recueil de renseignement, après avis de la CNCTR.

l'amendement, M. Olivier Cadic [(1)], de tels dispositifs créeraient des vulnérabilités exploitables par des cybercriminels ou des États hostiles.

L'examen comparé des expériences étrangères confirme par ailleurs l'absence, à ce jour, de modèle stabilisé pour l'accès aux messageries cryptées. Au Royaume-Uni, bien que l'*Investigatory Powers Act* de 2016 permet au gouvernement britannique d'exiger des opérateurs la mise en place de dispositifs techniques destinés à satisfaire les demandes d'interception, les démarches visant à obtenir un accès effectif aux communications chiffrées n'ont, à ce jour, pas abouti. À deux reprises en 2025, le gouvernement britannique a adressé à l'entreprise *Apple* une réquisition visant à obtenir un accès aux données et messages cryptés des utilisateurs britanniques stockés sur le service iCloud. L'entreprise a retiré certaines fonctionnalités supplémentaires de chiffrement pour les utilisateurs britanniques, mais elle n'a toutefois pas modifié l'architecture de son système, comme exigé, réaffirmant publiquement son refus de créer une porte dérobée [(2)].

L'accès aux contenus chiffrés demeure pourtant un enjeu opérationnel majeur pour les services de renseignement, dans un environnement où 60 % à 80 % des communications transitent désormais par des applications de messagerie chiffrées de bout en bout, tandis que l'usage des SMS et des appels téléphoniques traditionnels reculent. La réflexion sur les modalités d'accès dépasse, par ailleurs, le seul cadre national. À l'échelle de l'Union européenne, la stratégie *ProtectEU*, présentée en avril 2025, prévoit la publication en 2026 d'une feuille de route sur le chiffrement afin d'identifier et d'évaluer les solutions permettant un accès légal aux données chiffrées par les autorités compétentes [(3)].

À l'évidence, les conditions de préparation du débat parlementaire sur le sujet du chiffrement, particulièrement à l'Assemblée nationale, n'ont pas permis de dépasser des postures politiques de principe. C'est regrettable car les débats auraient pu prendre une orientation différente si l'exécutif et les services de renseignement – qui ont besoin d'accéder aux contenus des communications cryptées pour mener leurs enquêtes – avaient présenté les choses avec plus de clarté à la représentation nationale. Il semble nécessaire de remettre le métier sur l'ouvrage et, dès lors que le sujet sera clarifié sur la technique envisagée par les services, la Délégation prendra toute sa part au travail de pédagogie nécessaire auprès des parlementaires pour légiférer en connaissance de cause.

---

(1) Amendement n° 1 rectifié quinquies, déposé par M. Olivier Cadic, visant à ne pas imposer aux fournisseurs de services de chiffrement l'intégration de dispositifs techniques visant à affaiblir volontairement la sécurité des systèmes d'information et des communications électroniques.

(2) The Guardian, « UK government resumes row with Apple by demanding access to British users' data », *1er octobre 2025.*

(3) Commission européenne, Feuille de route pour un accès licite et effectif aux données à des fins répressives, *24 juin 2025.*

2. Le recours à la technique de renseignement algorithmique

L'article 15 de la loi déférée devant le Conseil constitutionnel visait à étendre, à titre provisoire, la technique de renseignement algorithmique à la détection des menaces liées à la criminalité et à la délinquance organisées punies de dix ans d'emprisonnement, en tant qu'elles concernent le trafic de stupéfiants et d'armes ainsi que le blanchiment des produits qui en sont issus. Cette technique repose sur l'analyse de grands volumes de données de connexion afin d'identifier des motifs révélateurs d'une activité criminelle.

Alors limité à la prévention du terrorisme, le recours à cette technique avait déjà été étendu en 2024, à titre provisoire et jusqu'au 1er juillet 2028, pour les finalités liées à l'indépendance nationale, l'intégrité du territoire et la défense nationale (1° de l'article L. 811-3 du code de la sécurité intérieure), aux 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 (2° du même article) [(1)].

Cette technique a également connu en 2021 un élargissement de ses modalités de mise en œuvre. La loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement avait, en effet, étendu le champ de ces traitements aux « *adresses complètes de ressources utilisées sur internet* », c'est-à-dire aux URL, sans que le Conseil constitutionnel ne se prononce alors sur ce point.

Dans le cadre de sa saisine sur la loi dite « narcotrafic », le Conseil constitutionnel a finalement estimé que cette extension ne ménageait pas un équilibre suffisant entre les objectifs de prévention des atteintes à l'ordre public et le droit au respect de la vie privée. Il a relevé que les adresses URL constituent des « données mixtes » susceptibles de comporter à la fois des éléments de connexion et des termes renvoyant au contenu de correspondances échangées ou d'informations consultées. Or, le dispositif prévoyait l'utilisation de ces adresses de manière générale et indifférenciée, sans condition tenant à la nature des données révélées. L'article 15 de la loi a, en conséquence, été déclaré contraire à la Constitution.

Par application de sa jurisprudence « Nouvelle-Calédonie », le Conseil a, par ailleurs, étendu ce raisonnement à la disposition déjà en vigueur de l'article L. 851-3 du code de la sécurité intérieure, qui autorisait le traitement algorithmique d'URL pour les autres finalités. Il s'agit ainsi d'une remise en cause plus large du cadre juridique applicable aux algorithmes, au-delà du seul texte déféré.

Le Conseil constitutionnel n'interdit pas, pour autant, par principe le recours aux traitements algorithmiques fondés sur les URL, mais il exige qu'ils soient assortis d'un encadrement législatif sensiblement plus précis.

---

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

Cette décision souligne la sensibilité particulière que revêt la régulation des techniques de renseignement les plus sophistiquées : la nature des données traitées, le volume d'informations analysées, le niveau de granularité ainsi que les capacités de corrélation algorithmique imposent au législateur un calibrage rigoureux, fondé sur une appréhension fine des paramètres de conception.

CHAPITRE III :
LA TRANSFORMATION DU RENSEIGNEMENT FRANÇAIS FACE AUX RUPTURES DU MONDE

Les bouleversements géopolitiques et la vitesse de transformation du monde placent le renseignement au cœur des équilibres stratégiques. Multiplication des foyers de crise, contestation de l'ordre international, hybridation des menaces : les repères établis depuis la fin de la guerre froide se brouillent. Les ruptures technologiques, la compétition informationnelle et la porosité croissante entre enjeux militaires, économiques et sociétaux bouleversent les méthodes d'anticipation. Dans ce contexte mouvant et fragmenté, les services de renseignement doivent repenser leurs approches, leurs partenariats et leurs capacités d'analyse.

Dans cette ère nouvelle qui s'ouvre, l'existence d'un renseignement doté de capacités autonomes constitue un enjeu majeur pour continuer à jouer dans la cour des grands, assurer notre sécurité nationale et garantir l'exercice effectif de notre souveraineté. Le cadre légal établi en 2015 a posé les fondations d'une architecture juridique solide, définissant les finalités, les techniques autorisées et les modalités de contrôle des services. Dix ans après son adoption, l'évolution rapide des menaces, la sophistication des technologies et la transformation du paysage informationnel ouvrent de nouvelles questions juridiques. Cette réflexion s'inscrit désormais dans un environnement européen et international où l'interdépendance des États impose plus que jamais une coopération fondée sur le discernement, l'efficacité et le pragmatisme.

I. L'ADDITION DES MENACES, DANS UN MONDE DE CONFRONTATIONS, CONFÈRE AU RENSEIGNEMENT UN RÔLE DÉCISIF DANS L'EXERCICE DE NOTRE SOUVERAINETÉ

La période actuelle est singulière en ce qu'elle impose de faire face simultanément à une prolifération des menaces qui se situent toutes à un haut niveau d'intensité.

A. LES MENACES S'ADDITIONNENT ET SE RENFORCENT

Longtemps appréhendées comme des phénomènes successifs, laissant aux États le temps d'adapter leurs réponses, les menaces contemporaines ne s'inscrivent plus dans une logique de succession mais d'addition et d'imbrication. Terrorisme, ingérences étrangères, criminalité organisée, cyberattaques, instabilité géopolitique et enjeux technologiques se renforcent désormais mutuellement, créant un environnement stratégique d'une complexité inédite pour la France comme pour l'Europe. **Cette superposition de risques hétérogènes, mêlant acteurs étatiques et non étatiques, espaces physiques et numériques, impose une transformation profonde de l'action publique en matière de sécurité nationale**. Face à cette réalité, les services de renseignement deviennent un pivot essentiel : ils doivent non

seulement détecter et anticiper des menaces multiples, mais aussi comprendre leurs interactions pour éclairer la décision politique et protéger durablement notre société.

1. La persistance de menaces « classiques » impactées par le contexte géopolitique

a. La permanence d'une menace terroriste qui se nourrit des crises internationales

La menace terroriste est passée d'un niveau extrême en 2015, caractérisée par un phénomène massif de départs du territoire national vers la Syrie, auprès de l'État islamique, à une menace qui demeure durablement élevée, dans un contexte certes d'affaiblissement structurel d'Al Qaïda et de l'État islamique (EI) mais néanmoins de permanence de réseaux jihadistes cherchant à frapper le territoire national et les intérêts français.

Force est de constater une grande sensibilité du niveau de la menace terroriste à des facteurs externes aux sujets nationaux. **La menace terroriste qui pèse sur la France et sur l'Europe est directement corrélée aux évolutions géopolitiques** qu'il s'agisse des coups d'État au Sahel depuis 2019, du retour au pouvoir des Talibans en Afghanistan en août 2021, du déclenchement de la guerre en Ukraine en février 2022 et du conflit entre Israël et le Hamas depuis le 7 octobre 2023.

Le rapprochement dans le temps et parfois la combinaison de ces crises ont contribué à une évolution de la physionomie de la menace terroriste au cours de la période récente. Coutumières de l'instrumentalisation de l'actualité internationale pour faire valoir leur idéologie respective, l'EI et Al Qaïda s'en sont saisies pour véhiculer leurs narratifs, mettant aussi en exergue leurs divergences. Pour l'EI en particulier, chaque événement saillant de l'actualité internationale, qu'il ait ou non trait à l'islam ou aux enjeux du monde arabo-musulman, est interprété comme un signe de la décadence ou de l'immoralité du monde occidental, et, par extension, comme une preuve de la validité de son dogme.

Au-delà de la récupération de la situation géopolitique pour avaliser leur propre agenda, **les organisations terroristes ont, *in fine*, fait de chaque crise internationale un prétexte pour recentrer leur discours sur la lutte contre l'Occident et appeler à le frapper.**

En 2021, le communiqué d'Al Qaïda central célébrant la victoire des Talibans en Afghanistan se concluait par un appel à la libération des terres de Jihad, notamment du Maghreb islamique, dénonçant plus spécifiquement « *l'occupation française* ».

En 2022, les deux organisations terroristes ont appelé à utiliser le *momentum* créé par la guerre en Ukraine pour frapper l'Europe. C'est ainsi que le Jaysh-al-Malahem al-Electroni *via* son magazine Wolves of Manhattan, identifiait les moyens par lesquels les jihadistes pourraient capitaliser sur le conflit à des fins terroristes. L'organe pro-AQ suggérait notamment aux « *loups solitaires* »

d'investir la guerre afin d'y bénéficier de formations militaires et y constituer des cellules terroristes et des caches d'armes. Dans la même logique, l'EI, par la voix de son porte-parole Hajji Aballah le 17 avril 2022, exhortait ses partisans à tuer les « *mécréants et les juifs* » en saisissant l'opportunité de la guerre entre « *croisés* » pour commettre des attentats dans une Europe particulièrement vulnérable.

Enfin, la dégradation continue de la **situation sécuritaire en Afrique sahélienne** augmente elle aussi la menace terroriste contre les intérêts français. À moyen terme, elle présente le risque de la reconstitution de capacités de projection de la menace vers l'Europe.

Dix ans d'évolution de la menace terroriste

Au cours de la décennie écoulée, la menace terroriste a évolué mais son intensité demeure très élevée.

En 2016, la diminution des capacités de projection de l'EI a entraîné un basculement vers une menace principalement soutenue depuis la zone syro-irakienne ou inspirée par la propagande de l'organisation terroriste.

Entre 2017 et 2019, la menace a été incarnée par des acteurs endogènes inspirés par l'EI, permettant à l'organisation terroriste de capitaliser sur les actions menées en son nom pour préserver son image de marque tandis qu'elle accumulait les revers militaires.

Entre 2020 et 2022, un phénomène d'autonomisation de la menace s'est traduit par la multiplication d'attentats commis par des individus évoluant en périphérie, voire en dehors de la menace jihadiste traditionnelle et réagissant à des thématiques sensibles (blasphème, islamophobie).

Depuis 2023, les projets d'action violente ont majoritairement été portés par de jeunes acteurs endogènes pro-EI, moins marqués idéologiquement que leurs prédécesseurs et évoluant principalement dans l'espace virtuel.

La reprise du conflit israélo-palestinien en octobre 2023 et la chute inattendue du régime de Bachar Al-Assad en Syrie en décembre 2024 ont constitué des bouleversements géopolitiques majeurs ayant d'ores et déjà influé sur l'évolution de la menace jihadiste nationale.

b. La force de frappe inédite des réseaux de la criminalité organisée

Les organisations criminelles se transforment et ont accès à **des moyens de plus en plus sophistiqués, qui font d'elles de véritables compétiteurs pour les États**. Cette évolution, dont les effets déstabilisateurs se mesurent déjà dans certains pays d'Amérique latine, s'installe progressivement en Europe (Espagne, Pays-Bas, Belgique), au risque d'une mise en péril de la sécurité et de la capacité des États à conserver la maîtrise de leur territoire.

La force de frappe des organisations criminelles dites du « haut du spectre » est un motif de préoccupation pour les services de renseignement. Elles s'adaptent de plus en plus rapidement aux mesures de surveillance avec un investissement de plus en plus efficace dans les nouvelles technologies et les évolutions logistiques,

comme l'utilisation de narco-submersibles traversant l'Atlantique à l'aide d'un guidage automatique. Elles disposent désormais de capacités technologiques qui ont longtemps relevé d'un monopole de la puissance publique (tags, balises, drones, messageries cryptées, téléphones satellitaires, etc.) leur permettant de rivaliser avec les capacités des forces de l'ordre.

Cette montée en puissance capacitaire des réseaux criminels vient remettre en cause **l'asymétrie des moyens** dont bénéficient historiquement les services régaliens.

Mise en œuvre de techniques de surveillance des services, dépoussiérage des zones de rendez-vous, développement de contacts au sein des professions d'intérêt en vue d'accéder à des données ou des sites, maîtrise des outils informatiques : la connaissance fine dont les réseaux criminels disposent du fonctionnement des infrastructures stratégiques de la chaîne logistique et des méthodes de contrôle des services répressifs, leur permet d'en exploiter les faiblesses et d'adapter leurs modes opératoires en conséquence tant sur les plans technique que logistique.

Les failles de sûreté au sein des infrastructures portuaires facilitent les trafics, en particulier celui de la cocaïne en provenance d'Amérique latine. Elles présentent autant d'opportunités d'accès pour les réseaux criminels, leur surface financière permettant en outre l'utilisation d'un degré d'équipement technique croissant. Le renforcement des mesures de sécurité dans les ports et la digitalisation de la chaîne logistique pourraient inciter les groupes criminels à cibler de nouveaux profils. Ils pourraient notamment avoir recours à des *hackers* afin de pirater les logiciels de contrôles et d'organisation des flux marchands au sein des ports, ou encore renforcer la corruption d'agents publics.

Les services de renseignement constatent le recours croissant, par les organisations criminelles, à la création ou à l'usurpation de l'identité de sociétés réelles pour le trafic de produits stupéfiants par fret aérien ou maritime conteneurisé. Les marchandises illicites font l'objet de transactions entre des sociétés sans activités commerciales réelles, mais d'apparence légale. Ces entités économiques « fantôme » se fondent dans la masse des flux internationaux et s'avèrent très difficiles à détecter.

Afin d'opacifier leur activité criminelle, le *dark web*, les réseaux sociaux et messageries cryptées sont employés pour couvrir l'ensemble des étapes des trafics, notamment la vente des produits illicites et le blanchiment des revenus procurés. Après avoir investi la dimension cyber et les cryptomonnaies, le développement de l'économie collaborative et de l'intelligence artificielle offre aux réseaux criminels de nouvelles opportunités (flux fictifs *Vinted, AirBnB* servant de lieux de stockage transitoire, etc.).

Au final, les organisations criminelles cherchent à saturer les capacités de traitement du renseignement douanier, soit par la massification et la fragmentation des envois, soit par la qualité de la dissimulation.

c. Les atteintes répétées à la sécurité économique

Le rapport Roux de Bézieux sur la sécurité économique des entreprises, remis en septembre 2024 au Président de la République, révèle qu'environ un millier d'alertes d'ingérences économiques ont été recensées en France en 2023, soit un volume multiplié par trois depuis 2020. Les traitements d'alertes par le Service de l'Information Stratégique et de la Sécurité Économique (SISSE) ont augmenté d'environ 40 %. Le rapport met l'accent sur l'extension des secteurs concernés : les technologies critiques et les unités de recherche scientifique sont désormais dans le « référentiel » de la sécurité économique. La menace ne vise plus seulement les grandes entreprises mais concerne désormais largement les PME et les ETI.

Notre base industrielle et technologique de défense (BITD) est une cible privilégiée de puissances étrangères. ***** les actions hostiles ont gagné en fréquence mais aussi en diversité. La DRSD a ainsi constaté l'instrumentalisation croissante du droit à travers l'extraterritorialité et l'instrumentalisation des normes. À l'horizon 2030-2035, la menace posée par l'extraterritorialité du droit ***** va aller croissant, augmentant d'autant plus la prédation sur les entreprises françaises. Les services de renseignement étrangers, *****, agissant de plus en plus de façon désinhibée, pourraient devenir encore plus agressifs sur le territoire national.

On observe en particulier **une exposition accrue des entreprises impliquées dans le soutien militaire à l'Ukraine.** Cela rend nécessaire un accompagnement renforcé des entreprises relevant de l'économie de guerre, à savoir celles considérées comme indispensables au renforcement de la capacité de la France à participer dans la durée à des combats de haute intensité. En 2024, en liaison avec la Direction générale de l'armement (DGA) et les principaux maîtres d'œuvre industriels, ***** des entreprises identifiées ont fait l'objet d'un accompagnement de la DRSD sur le volet de la protection physique et ***** sur le volet cybersécurité.

2. La prolifération de nouvelles menaces hybrides et transversales

a. Des modes opératoires protéiformes

Les **menaces hybrides** désignent des stratégies hostiles qui combinent plusieurs moyens d'action – militaires, économiques, politiques, cybernétiques, informationnels – pour déstabiliser un État ou une organisation sans franchir clairement le seuil d'un conflit ouvert. Elles mêlent par exemple désinformation, cyberattaques, pressions économiques, actions clandestines ou exploitation de tensions sociales. L'objectif est de créer de la confusion, affaiblir la cohésion

d’un pays et influencer ses décisions, tout en rendant difficile l’attribution de l’attaque et la réponse à y apporter.

L’Europe est confrontée depuis une quinzaine d’années et, singulièrement depuis le début de l’agression russe en Ukraine, à **un accroissement et une diversification de ces modes d’action, sans qu’il soit toujours possible de les attribuer formellement à une puissance étrangère hostile**. C’est notamment le cas des survols de drones, d’origine officiellement inconnue, observés depuis l’automne 2025 au-dessus de plusieurs aéroports européens – civils comme militaires – provoquant des fermetures temporaires, des détournements d’avions ou des annulations de vols.

Couvrant un vaste spectre de menaces, allant de l’espionnage à l’influence hostile, des puissances étrangères consacrent à ces activités des moyens humains et techniques considérables, qui ne se cantonnent plus seulement à la captation d’informations et se caractérisent de plus en plus par des interventions dans les affaires intérieures de l’État, dans le but d’affaiblir, d’infléchir ou de déstabiliser sa politique ou son positionnement sur la scène internationale.

La période actuelle est marquée par un changement d’échelle dans la nature et l’intensité des ingérences russes. Si la Russie a maintenu depuis les années 2000 une politique agressive d’espionnage et d’influence contre les intérêts français, elle a considérablement accru ses attaques indirectes, notamment dans le champ informationnel, d’abord en Afrique sahélienne à compter de 2017-2018, puis de manière extensive au gré de l’affirmation du soutien français à l’Ukraine.

Démonstrations de force, attaques informatiques à des fins d’espionnage, de sabotage d’infrastructures critiques ou de déstabilisation, pression sur les ressources énergétiques, pression sur les flux migratoires, ingérence et lutte informationnelle : dans un contexte géopolitique où nombre de puissances adverses opèrent contre les intérêts français d’une façon totalement décomplexée, cette menace protéiforme représente un réel défi pour les services de renseignement qui doivent recourir de manière accrue à des mesures d’entrave administrative, voire judiciaire. La mise en œuvre de mesures concertées de *persona non grata* (PNG) contre les officiers russes en réponse à l’affaire *Skripal* ou à l’invasion russe de l’Ukraine a ainsi permis d’affaiblir substantiellement le dispositif des services de renseignement russes en Europe.

b. L’espace numérique, champ de bataille de la guerre informationnelle

Selon Viginum, chargé de la vigilance et de la protection contre les ingérences étrangères, pas moins de **25 opérations numériques menées par des acteurs étrangers ont été détectées au cours de l’année 2024**. L’organisation par la France des Jeux Olympiques et Paralympiques à l’été 2024 a fait de notre pays une cible prioritaire. Entre avril 2023 et le 8 septembre 2024, date de fin des Jeux, Viginum a ainsi identifié 43 manœuvres informationnelles ayant spécifiquement ciblé les Jeux de Paris 2024.

Les **campagnes électorales** sont également dans le viseur des puissances étrangères et de leurs *proxies,* comme l'ont montré les manipulations de l'information ayant ciblé l'élection présidentielle roumaine de 2024, dont les résultats du premier tour ont été annulés par la Cour constitutionnelle roumaine. C'est bien le bon fonctionnement de nos démocraties qui est en jeu.

Depuis la fin de l'année 2023, Viginum observe et documente les activités d'un mode opératoire informationnel (MOI) russe susceptible d'affecter le débat public francophone et européen. Connu en source ouverte sous le nom de « Storm-1516 », ce MOI est actif *a minima* depuis l'été 2023. Il est responsable de plusieurs dizaines d'opérations informationnelles ayant ciblé des audiences occidentales, dont françaises.

Selon le rapport de Viginum, l'objectif principal de Storm-1516 semble être avant tout de décrédibiliser le gouvernement ukrainien, probablement ans l'espoir d'entraîner la suspension de l'aide occidentale à l'Ukraine. En parallèle, le MOI cible directement des dirigeants européens et leur entourage, notamment durant les périodes électorales en France, aux États-Unis et en Allemagne. Pour ce faire, le mode opératoire diffuse généralement des *deepfakes*.

Les investigations de Viginum, qui s'appuient notamment sur des éléments révélés en source ouverte, confirment l'implication d'individus et d'organisations proches du gouvernement russe, dont John Mark Dougan, un ancien policier américain exilé en Russie, ainsi que de membres des écosystèmes Prigojine et Douguine.

La répétition de ces ingérences est, selon Viginum, la marque d'une « *intention qui se déploie sur le long terme, de saper la cohésion, discréditer les institutions et modifier les perceptions sur notre modèle démocratique* ». Les nouveaux sujets de clivage (dérèglement climatique, immigration de réfugiés climatiques, égalité femme-homme) sont appelés à être de plus en plus utilisés pour fracturer l'opinion publique occidentale.

La technologie, en particulier l'intelligence artificielle, permet désormais de mener des campagnes d'ingérence informationnelle de grande ampleur, appuyant sur les divergences d'une société de plus en plus polarisée, et instrumentalisant la population pour créer de la défiance vis-à-vis des institutions étatiques. Le nombre croissant et les disponibilités des outils d'attaque vont démocratiser l'accès aux opérations de lutte informatique active (LIA) à grande échelle, qui demeuraient jusqu'alors l'apanage des États et de quelques grands groupes criminels. Des groupes terroristes ou activistes, même faiblement structurés, auront probablement à leur disposition, dans un futur proche, des arsenaux efficaces, parfois appuyés sur des chaînes automatisées grâce à l'intelligence artificielle pour gagner en réactivité et en efficacité.

B. LES RUPTURES GÉOPOLITIQUES MOBILISENT LA COMMUNAUTÉ DU RENSEIGNEMENT

La nouvelle donne géopolitique clôt le chapitre de l'après-guerre froide et marque l'entrée dans une ère nouvelle de confrontation systémique où la compétition entre les puissances, la remise en cause du multilatéralisme et la banalisation de la violence constituent le nouveau cadre d'action. Ces ruptures géopolitiques à l'œuvre et les conflits en cours ont un impact immédiat et durable sur l'activité des services de renseignement.

1. L'adaptation du dispositif et des missions du renseignement au contexte international

a. La nouvelle donne en Afrique et ses conséquences sur la carte des implantations françaises

Les coups d'État militaires survenus au Sahel depuis 2021 ont rebattu les cartes de la présence française dans cette partie de l'Afrique. *****.

L'Afrique subit une fragilité structurelle qui, si elle n'est pas nouvelle, s'aggrave du fait de la montée en gamme qualitative des armements en circulation sur le continent, de la contestation et de l'affaiblissement du système international dans de nombreux pays de la région, et enfin de la difficulté des organisations régionales à contenir les conflits et à réguler les tensions sécuritaires du continent. Les conflits deviennent ainsi plus violents et tendent à se sous-régionaliser. Ces fragilités sont favorables à l'extension des groupes terroristes, qui profitent des déliquescences étatiques pour conforter leurs sanctuaires et poursuivre leur essor, ainsi qu'à l'action de nos compétiteurs – essentiellement la Russie et la Chine et dans une moindre mesure la Turquie – qui exploitent cette nouvelle permissivité du continent africain afin de promouvoir leurs intérêts de façon pragmatique et dénuée de toute idéologie.

L'Afrique demeure toutefois une zone d'intérêt et de déploiement majeur tant pour la DGSE que pour la DRM qui doit continuer à produire du renseignement permettant de préparer les décisions militaires du CEMA, d'appuyer nos opérations militaires et d'accompagner nos partenaires africains. Renseigner sur le continent africain impose, plus que par le passé, d'adopter une approche *ad hoc* compte tenu de la situation sécuritaire, ainsi que de l'évolution de notre posture militaire en Afrique, qui se veut **moins visible et plus agile.**

Dans le cadre de l'évolution du contexte stratégique en Afrique et de la mise en œuvre du plan « Faire autrement avec l'Afrique », *****.

b. Des redéploiements liés aux conflits en cours

La DRSD, chargée de protéger nos forces déployées sur des théâtres d'opérations extérieures, a ajusté à la menace son empreinte géographique hors du territoire national ***** accompagnant le mouvement des forces armées. *****.

Dans un contexte de forte médiatisation de la guerre en Ukraine, ce service s'est attaché à prévenir les éventuels débauchages, à entraver les départs en zone de combats ***** ; elle participe plus largement à l'évaluation des menaces susceptibles de viser la sphère de défense élargie depuis son engagement en soutien à l'Ukraine.

*******.** Le Service a également pu fournir des appuis en matière de contre-ingérence aux déploiements du Groupe aéronaval, à bord et lors d'escales majeures. La formation des agents doit elle aussi s'adapter en conséquence, prenant en compte des contraintes nouvelles *****.

c. De nouvelles missions assignées aux services de renseignement

La plupart des services de renseignement voient leurs activités sérieusement impactées par le contexte géopolitique.

Alors que l'agression russe en Ukraine donne lieu à des vagues successives de sanctions occidentales (économiques, commerciales et financières), la DNRED est impliquée au quotidien dans la mise en œuvre opérationnelle des gels ou saisies d'avoirs russes en France ; elle concourt, avec d'autres services comme Tracfin, à la mission de lutte contre le contournement des sanctions qui passe par la détection de différents phénomènes de fraudes, dont ceux des *personal shoppers* [(1)] et de la fraude à la détaxe impliquant des individus de nationalité russe. Le renseignement douanier surveille aussi la menace d'une dissémination d'armes à destination du territoire national, provenant de la guerre en Ukraine. Pour l'heure, aucune saisie ni contrôle n'ont toutefois permis d'affirmer l'émergence d'un trafic d'armes important depuis l'Ukraine.

La DRSD est pour sa part chargée d'évaluer les impacts directs et indirects de ces sanctions sur la BITD (approvisionnements, activités commerciales, partenariats). En matière de protection contre ces menaces, la DRSD a consacré une part de son activité au volet sécuritaire du modèle d'économie de guerre. En liaison avec la DGA et les grands maîtres d'œuvre industriels, ce service a proposé un accompagnement spécifique à des entreprises identifiées comme les plus stratégiques et dont la criticité repose essentiellement sur la non-substitualité de leur activité sur le territoire national. Dans ce cadre, sur la base de référentiels de sûreté physique et de maturité cyber, la DRSD a mené des actions d'évaluation auprès ***** de sous-traitants de la BITD et mis en œuvre un processus d'accompagnement et de conseil individualisés.

Au Proche et Moyen-Orient, la chute surprise du régime d'Assad en Syrie en décembre 2024 a conduit Tracfin ***** une vigilance accrue d'une part sur les risques de mouvements de capitaux d'entités sanctionnées et d'autre part sur les risques de reconstitution de la menace terroriste sur le territoire syrien et dans

---

(1) Les « personal shoppers *» sont des individus qui effectuent des achats sur le territoire national pour le compte de clients domiciliés à l'étranger, en l'espèce des individus russes.*

la région. La priorité accordée à la Syrie a été rehaussée et donne lieu à des travaux en renseignement ainsi qu'avec l'autorité judiciaire.

Si le changement de régime n'a pas eu d'effet direct sur l'arrivée de produits stupéfiants en France, d'importantes saisies, notamment de captagon, ont été réalisées par des services douaniers de la zone en coopération avec la DNRED.

2. La définition d'une nouvelle doctrine qui confère un rôle central aux services de renseignement face à la dangerosité du monde

a. La nouvelle Revue nationale stratégique (RNS)

Auditionné le 26 juin 2025 par la Délégation, le secrétaire général de la défense et de la sécurité nationale a présenté les principales orientations de la nouvelle *Revue nationale stratégique* (RNS) alors en cours de finalisation. Ce document procède à une mise à jour de la doctrine française au vu de la dégradation de l'environnement international. **Cette formalisation de la doctrine française prend un relief particulier au lendemain de la publication par les États-Unis, le 5 décembre 2025, de leur nouvelle stratégie de sécurité nationale, qui marque une rupture nette avec le paradigme transatlantique d'après 1945.** Ce texte met l'accent sur la protection des « intérêts nationaux fondamentaux » américains, et affirme que Washington n'interviendra plus systématiquement dans les affaires mondiales, sauf si ces intérêts sont directement menacés.

L'Europe est directement visée : la stratégie dépeint le vieux continent comme affaibli, menacé d'un « effacement civilisationnel » en raison de l'immigration, de la baisse des natalités et de ce qu'elle considère comme des dérives politiques ou culturelles. Le document appelle aussi les pays européens de l'OTAN à accroître massivement leurs dépenses militaires pour compenser le désengagement américain. À l'opposé de la RNS française qui repose sur un **scenario central** (1), celui d'un conflit avec la Russie, la stratégie américaine minimise la menace posée par Moscou.

La *Revue nationale stratégique* française réaffirme quelques priorités majeures. D'abord, la nécessité de préserver une dissuasion nucléaire robuste, pilier ultime de la souveraineté. Ensuite, la modernisation accélérée des armées pour affronter des conflits plus intenses, faire face à des adversaires technologiquement avancés et protéger l'autonomie stratégique française dans un contexte de compétition industrielle mondiale.

La revue insiste également sur la valeur des alliances, en particulier l'OTAN, qui retrouve un rôle central dans la défense collective européenne. Mais elle souligne que la France doit simultanément renforcer sa liberté d'appréciation et

---

(1) Ce scénario central est précisé en ces termes au point 112 de la RNS : « L'hypothèse d'une participation des armées françaises à une guerre majeure de haute intensité dans le voisinage de l'Europe et le risque d'actions concomitantes déstabilisatrices de nature hybride pour la sécurité intérieure de la France atteignent un niveau inégalé depuis la fin de la guerre froide. La menace d'une guerre conventionnelle majeure sur le territoire national hexagonal n'est en revanche pas considérée comme crédible ».

d’action, ce qui suppose une souveraineté industrielle, technologique et informationnelle accrue.

Au sein de cette stratégie, le renseignement est présenté comme un multiplicateur stratégique essentiel. Dans un monde où la surprise stratégique est redevenue possible, la France doit disposer d’une capacité d’anticipation supérieure, fondée sur une combinaison d’outils technologiques avancés, de présence humaine et de coopération accrue.

La RNS assigne les priorités suivantes à la communauté du renseignement :

– **Renforcer la maîtrise de l’information** : La compétition se joue d’abord dans la connaissance fine des intentions, des capacités et des vulnérabilités adverses. Les services doivent accroître leur autonomie analytique, croiser davantage renseignement technique, spatial, cyber et renseignement humain, et développer des capacités d’analyse massive de données.

– **Accélérer la transformation technologique** : Les ruptures liées à l’IA, au quantique, à la guerre algorithmique et aux capteurs de nouvelle génération modifient radicalement la nature du renseignement. La France doit investir pour ne pas dépendre de technologies étrangères et pour automatiser ce qui peut l’être, tout en préservant le rôle critique de l’expertise humaine dans l’interprétation et l’anticipation.

– **Protéger l’espace informationnel national** : Face aux opérations d’influence hostiles, à la manipulation des opinions et aux campagnes de désinformation, les capacités de détection, d’attribution et de réponse doivent être renforcées. Le renseignement joue ici un rôle clé dans l’exposition des ingérences étrangères.

– **Élargir la présence mondiale et la profondeur stratégique** : Le positionnement géographique des services – en Afrique, au Moyen-Orient, en Asie – doit s’adapter à la redistribution des zones de crise et à la montée des rivalités dans l’Indopacifique. La coopération européenne et la coordination avec les alliés demeurent essentielles, mais doivent être équilibrées par une capacité nationale autonome.

– **Sécuriser les chaînes logistiques et les infrastructures critiques** : La guerre économique et technologique est désormais centrale. Le renseignement économique et scientifique devient un enjeu prioritaire pour prévenir captations, dépendances, intrusions et sabotages.

Dans ce nouvel environnement international toujours plus instable, plus conflictuel et pétri d’incertitudes, le renseignement n’est plus seulement un outil d’appui : il devient la condition de la souveraineté décisionnelle et la première ligne de défense face aux menaces hybrides et aux puissances hostiles.

b. La mise à jour de la stratégie nationale du renseignement

La Stratégie nationale du renseignement (SNR) actualisée en janvier 2025 constitue la feuille de route de la communauté française du renseignement, sous la coordination du CNRLT. En cohérence avec la RNS, elle traduit de façon plus opérationnelle ce double mouvement de prise en compte d'un environnement géopolitique beaucoup plus instable et d'une montée en puissance des services de renseignement comme outil central de protection de la Nation.

Face à la nature désormais multidimensionnelle et hybride des menaces, la SNR fait du renseignement un instrument central de résilience nationale, chargé d'assurer la souveraineté décisionnelle de l'État et la protection des intérêts fondamentaux de la Nation.

Il est ainsi demandé aux services de renseignement de :

– **Produire une appréciation autonome** des intentions et capacités des acteurs (États, groupes armés, entreprises stratégiques, organisations criminelles) ;

– **Repérer précocement les signaux faibles** de crises géopolitiques, économiques ou sociétales.

– **Nourrir en continu la décision gouvernementale**, y compris dans la perspective d'un conflit majeur en Europe, scénario central de la RNS.

La SNR insiste aussi sur la nécessité de partager, coopérer, agir pour notre sécurité en France, en Europe et dans le monde. Concrètement, cela se traduit par :

– **Un renforcement du travail interservices** au sein de la « communauté nationale du renseignement ».

– **Une intégration accrue avec les partenaires européens** (UE, OTAN, coopérations bilatérales), afin de traiter des menaces transfrontalières que sont le terrorisme, la cybercriminalité, les ingérences, le narcotrafic, etc.

– **Un dialogue renforcé avec les diverses administrations d'État** (police, justice, diplomatie, armées) et certains acteurs privés stratégiques.

Il est également demandé aux services de renseignement d'être des acteurs d'innovation technologique, ce qui suppose :

– **Une mutualisation de certaines capacités techniques**, avec une logique de maîtrise souveraine des outils (capteurs, traitements, chaînes de données) ;

– **Le développement d'écosystèmes** mêlant experts data, cryptographes, spécialistes du quantique, du cyber, de l'électronique, du traitement du signal, chimistes, linguistes, aux côtés des métiers « classiques » du renseignement.

– **L’adaptation permanente** face aux adversaires qui exploitent l’IA, le chiffrage, les plateformes numériques.

La SNR souligne enfin l’enjeu visant à attirer et à promouvoir les compétences au sein de la communauté du renseignement : montée en gamme des profils recrutés, gestion prévisionnelle des emplois, fidélisation des talents, diversification des parcours.

C. UN NOUVEAU CYCLE S’OUVRE POUR LE RENSEIGNEMENT FRANÇAIS

Addition des menaces, ruptures géopolitiques, technologiques et sociales, retour à une logique de confrontation : cette nouvelle donne ouvre clairement un nouveau cycle pour le renseignement français au moment où l’on observe un durcissement inédit des conditions opérationnelles dans lesquelles évoluent les agents des services de renseignement. Les arrestations récentes de membres de la DGSE (au Burkina Faso en 2023 et au Mali en 2025) illustrent une érosion des règles tacites de l’espionnage. Les États ciblent désormais ouvertement les agents étrangers, instrumentalisant ces affaires pour des gains diplomatiques ou de politique intérieure. Parallèlement les régimes autoritaires (Chine, Russie, Iran), qui sont nos cibles prioritaires, verrouillent leurs systèmes via des contre-mesures technologiques (IA de surveillance, cloisonnement numérique), un resserrement du processus de décision et une répression accrue des sources humaines, rendant la pénétration classique plus difficile.

1. De nouvelles méthodes de travail adossées à de profondes réorganisations internes

La plupart des services de renseignement ont mené des réformes en profondeur de leur organisation interne, **fondées sur le décloisonnement et la transversalité**, alors que l’essor de l’intelligence artificielle, la généralisation des données massives (big data) et l’hyper connectivité des sociétés ont redéfini les modalités de collecte, d’analyse et d’exploitation du renseignement.

a. La création de centres de mission à la DGSE

À la DGSE, le chantier de la réorganisation interne s’est engagé dès 2019. Il s’agissait alors de réfléchir aux pistes d’améliorations à apporter au modèle d’organisation du Service, qui n’avait, dans ses grandes lignes, pas évolué depuis les réformes du préfet Silberzahn à la fin des années 1980, autour de la mise en place de cinq grandes directions.

Rapidement, il est apparu que poser des rustines ne suffirait pas : le fonctionnement en silo, avec des directions spécialisées autour de savoir-faire, avait atteint ses limites. Le fonctionnement interne du Service était devenu trop lourd, ses coûts de coordination trop importants. Par ailleurs, il fallait s’adapter à la hausse exponentielle des renseignements recueillis, notamment d’origine technique.

La réforme, effective depuis le 1er novembre 2022, s'articule autour de plusieurs grands principes : subsidiarité, distinction entre responsabilité capacitaire et responsabilité de la mission, meilleure intégration des ressources et des compétences autour des missions. Au centre de la nouvelle organisation, se trouvent ******* centres de missions, ******* dont les chefs répondent directement au directeur général.

Les directions capacitaires, direction technique et de l'innovation et direction de la recherche et des opérations, mettent leurs capacités au service des centres de mission et imaginent les savoir-faire dont la DGSE aura besoin dans l'avenir. La direction de l'administration, quant à elle, est chargée de fournir à l'ensemble du Service les capacités humaines, financières, matérielles et immobilières dont il a besoin. Le Secrétariat général pour l'analyse et la stratégie agit en soutien de la direction générale pour le pilotage de la gouvernance stratégique en même temps qu'il a la responsabilité de la qualité des diffusions, du pilotage des relations partenariales et qu'il assume la mission prospective et anticipation.

Après trois années de recul**, un bilan positif est tiré de cette réorganisation**, considérée comme pertinente et adaptée à l'évolution de l'environnement opérationnel et international du Service. *****.

La DGSE adapte régulièrement son modèle pour améliorer l'efficience de son organisation. En 2025, les deux principaux chantiers ont été la création de la Direction de la sécurité et de la protection (qui regroupe au sein d'une seule entité des missions auparavant éparses) et la réorganisation de la DTI (qui passe d'une logique de capteurs à une logique de cibles), mieux armée pour pénétrer les cibles les plus difficiles.

b. Le projet stratégique 2030 de la DGSI

*****.

L'organisation interne de la DGSI a connu des évolutions récentes *****.

Le contexte actuel est en effet marqué par un double niveau de complexité, lié au cadre d'exercice de la mission avec des environnements techniques et juridiques en forte évolution et à un état de la menace se renforçant dans un cadre international très incertain (conflits déstabilisateurs, manipulation de l'information, hybridation des menaces, etc.). Pour faire face à ces exigences opérationnelles croissantes, l'organisation et le fonctionnement ***** doivent être adaptés pour lui permettre de renforcer sa capacité à intégrer et traiter les sujets stratégiques et transversaux, et à assurer les missions de représentation de haut niveau associées, tout en préservant la qualité d'expertise et de réactivité opérationnelle des sous-directions *****.

Les travaux viseront à ***** qui impose à la Direction d'être plus efficace et la perspective du déménagement programmé en 2029 dans le futur site unique de la sécurité intérieure à Saint-Ouen qui conduira le Service à gérer un bâtiment abritant plusieurs milliers de personnes.

c. La réforme « Valmy » de la DNRED

Entrée en vigueur le 1er septembre 2024, la réforme interne de la DNRED, réforme dite « Valmy », vise à une **vaste transformation de la structure centrale du service de renseignement douanier, accompagnée d'une mise à niveau numérique et immobilière et d'une rénovation de la politique RH**. La réforme entend répondre aux attentes des autorités et aux évolutions des menaces criminelles, en améliorant la qualité des analyses tout en renforçant ses capacités opérationnelles. Inspirée de celles qu'ont conduites d'autres services de renseignement – y compris à l'étranger – au cours des dernières années, elle substitue à la logique « métier » jusqu'à présent en vigueur, une logique « thématique ».

Auparavant, les agents de la DNRED étaient répartis selon leur statut. Cette organisation, utile au moment de la constitution du Service car elle permettait un haut degré de spécialisation des agents, a conduit à un silotage de sa structure qui peinait à créer des synergies et à penser en réseau alors même que l'état de la menace exige de réunir les différentes compétences sur une seule thématique (par exemple, le conflit russo-ukrainien et ses conséquences). Les directions « métiers » ont ainsi été supprimées le 1er septembre 2024 et remplacées par les directions thématiques suivantes :

– Une direction « lutte contre la criminalité organisée ».

– Une direction « lutte contre la délinquance économique et financière » qui accueille la nouvelle Unité de renseignement fiscal (URF), chargée de lutter contre les fraudes fiscales graves et complexes.

– Une direction de l'analyse.

– Une direction technique.

Ces quatre directions ont été complétées par une cinquième, créée le 1er septembre 2025 : la direction de l'administration qui réunit les différents services support auparavant directement rattachés au directeur de la DNRED.

Au sein de ces directions, les agents issus de tous les corps de métiers ***** sont répartis dans des départements centrés sur des thématiques regroupant l'ensemble des missions du service *****.

Une année après l'entrée en vigueur de la réforme, le Service indique porter un regard positif sur cette transformation interne. L'activité opérationnelle, point fort de la DNRED, reste soutenue : en témoignent des résultats toujours plus

importants, appuyés par une capacité d'analyse plus proche du terrain *****. La capacité analytique du Service a connu une nette amélioration avec une hausse importante de la production de notes à destination de la communauté du renseignement. D'un point de vue technique, la réforme est toujours en cours avec le déploiement progressif du réseau classifié du service au sein de ses différents échelons.

d. À la DRSD, la priorité donnée à la prospective

Face aux évolutions de la menace, la DRSD a procédé au renforcement de sa capacité prospective. Cette fonction est assurée au sein d'un bureau du Service qui s'y consacre à plein temps. Sa capacité d'analyse s'articule autour d'une évaluation des menaces à court, moyen et long terme, s'étendant sur une période de six mois à dix ans.

Les scénarios prospectifs sont élaborés sur la base de sources ouvertes et fermées provenant du milieu académique, des productions internes du Service ainsi que des notes transmises par les services de renseignement et entités partenaires. À partir de ces informations, les grandes tendances et évolutions en cours pouvant affecter la sphère défense sont identifiées. Les actions et déclarations des adversaires et des partenaires, la manifestation de signaux faibles ou encore l'émergence d'avancées technologiques sont analysées afin de dégager de potentielles menaces et vulnérabilités dans les domaines affectant son champ de compétence.

En complément, la DRSD a récemment développé une capacité de *red teaming*/*wargaming* visant à rassembler les agents du Service, sous format de *brainstroming* et ce, de façon décloisonnée et transverse. L'objectif est d'adopter le point de vue d'un compétiteur afin d'identifier et de discuter des cibles et modes d'action qu'il mettrait en œuvre pour exploiter les vulnérabilités des entités et du personnel de la sphère défense élargie à la BITD. Les sessions donnent lieu à des recommandations et restitutions afin d'améliorer l'action du Service, sa résilience ou son organisation.

e. Les méthodes de travail multicapteurs de la DRM

Pour faire face aux enjeux futurs, la DRM a mené à bien une transformation de son organisation interne à travers la création de plateaux rapprochant analyses, spécialistes de la recherche de renseignement et experts techniques, au service d'une production plus agile et efficace. La DRM s'appuie en outre sur la fonction interarmées du renseignement, forte de 8 000 personnes des commandements et unités du renseignement des armées, dans une logique de subsidiarité, réel démultiplicateur de capacité.

Toutes les manœuvres de recherche de la DRM étant désormais multicapteurs (orientation de capteurs dans tous les champs et les milieux et croisement des informations recueillies), les cycles du renseignement spécifiques à chaque domaine de recherche (ROIM-Renseignement d'origine image,

ROEM-Renseignement d'origine électromagnétique, ROC-Renseignement d'origine cyber, ROHUM-Renseignement d'origine humaine et Renseignement d'origine partenarial) sont maintenant imbriqués dans un cycle plus général qui constitue celui de la manœuvre globale. Cette complexité des manœuvres de recherche et l'exigence de coordonner et synchroniser de nombreux acteurs et capacités sont rendues nécessaires par l'évolution de nos adversaires et compétiteurs qui cherchent à dissimuler leurs intentions, voire à nous leurrer de manière active. Les bouleversements du contexte stratégique conduisent également la DPR à adapter en permanence son réseau de partenaires étrangers.

Les méthodes de travail évoluent aussi sans cesse pour s'adapter au volume toujours plus grand d'informations récoltées et à des outils d'exploitation et de capitalisation plus performants. Ainsi, grâce à une approche centrée sur la donnée, les analystes du renseignement militaire croisent toujours plus d'informations et de nature de plus en plus hétérogènes. C'est là une véritable révolution, qui accélère la partie « exploitation » du cycle du renseignement, qui permet de décloisonner de nombreux sujets et offre ainsi des perspectives nouvelles en matière d'analyse.

f. Les plateaux thématiques d'enquête mis en place par Tracfin

L'augmentation incessante du flux déclaratif, combinée à la complexification croissante des modes opératoires et des vecteurs financiers utilisés par les cibles du Service, rend nécessaire l'adaptation permanente du cycle du renseignement pratiqué par Tracfin. En effet, une croissance régulièrement actualisée des pratiques financières criminelles, selon les zones géographiques ou les vecteurs financiers employés, est indispensable pour permettre au Service de concentrer ses enquêtes sur les dossiers au plus haut potentiel d'impact.

Afin de répondre à ce besoin de connaissances, le Service teste régulièrement de nouvelles méthodes de travail, par exemple dans le cadre de plateaux thématiques d'enquête qui réunissent, pendant une durée déterminée, des enquêteurs de différents départements sur une thématique particulière. Les retours d'expérience réalisés permettent d'adapter les modes opératoires du Service et de capitaliser de la connaissance.

Tracfin a identifié ses prochaines priorités de transformation interne autour de :

– La sanctuarisation et la fidélisation des ressources humaines formées à la recherche de renseignements, à son exploitation et à son analyse.

– La formation continue de l'ensemble des enquêteurs aux technologies de la finance décentralisée et des crypto-actifs.

2. Une démarche renforcée de coopération interservices et de mutualisations

Toutes les composantes de la communauté du renseignement sont désormais engagées dans des dynamiques de coopération et de mutualisation, notamment au sein de la CNRLT dont le rôle est moteur pour fluidifier la coopération interservices.

L'intensité de la menace conduit en effet les services à approfondir leurs coopérations, aussi bien de façon bilatérale que de façon plus globale à travers des cellules interservices spécialisées, dont la plus-value est considérée comme majeure d'un point de vue technique. Les mutualisations sont porteuses d'émulation collective et viennent faciliter les parcours professionnels interservices.

Dans le domaine de la lutte contre le terrorisme, les différents services coopèrent avec la DGSI qui assure le chef de filât en la matière. Elle accueille en son sein l'EMaP (État-Major Permanent) où les membres de la communauté du renseignement affectent un agent de liaison permettant concrètement de croiser les connaissances de chacun.

En ce qui concerne la lutte contre le blanchiment et les fraudes fiscales, la DNRED travaille à actualiser le protocole de coopération qui lie la Direction générale des douanes et des droits indirects (DGDDI) à Tracfin. *****. Le renseignement douanier est également au cœur d'une coopération opérationnelle avec les services du second cercle, qui concerne tout à la fois l'entrave et le partage de renseignement. La DNRED entretient des relations privilégiées, notamment à l'échelle locale, avec ces services.

Dans cette logique de coopération interservices, les projets mutualisés permettent de **réaliser des économies d'échelle** par la rationalisation des dépenses et la concentration de l'expertise. Le partage des besoins entre services favorise aussi le développement d'outils plus adaptés et performants à long terme, répondant à des exigences communes plutôt qu'à des logiques cloisonnées. Surtout, la démarche de mutualisation se révèle cruciale pour les projets exigeants en ressources, comme ceux liés à l'intelligence artificielle, où la concentration des moyens de calcul – à la fois coûteux et rares – devient un levier stratégique.

a. Sur le plan technique

Plus spécifiquement en matière de renseignement technique, qui exige des ressources humaines et financières conséquentes, **les coopérations entre les directions techniques des services de renseignement ont atteint une phase de maturité**, qui permet des échanges de confiance, des projets de mutualisation et une circulation des ressources humaines.

Les directions techniques de différents services sont ainsi engagées depuis plusieurs années dans des groupes de travail sur des sujets techniques d'intérêt commun. *****.

De ces groupes de travail sont nés des projets d'intérêt majeur comme *****.

b. Sur le plan des ressources humaines

La coopération entre les directions techniques passe également par *****. Si, par le passé, changer de service était chose rare, cette pratique est aujourd'hui plus courante. Elle est source d'enrichissement des expériences et valorise les plus beaux parcours techniques.

Sur le plan des ressources humaines, de nombreuses actions ont ainsi été menées ces dernières années pour développer la coopération et la mutualisation entre les services, avec le concours de l'Académie du renseignement :

– Développement des formations dans le domaine du renseignement.

– Développement des mobilités interservices dans le cadre d'une charte de bonne conduite signée par les directeurs des services de renseignement.

– Établissement d'un référentiel de rémunération spécifique aux métiers du renseignement d'origine technique.

Si des défis persistent, notamment en matière de coordination, **le bilan demeure très favorable à une approche collaborative**. Tous les services dressent un bilan positif de cette démarche de mutualisation, au vu des gains d'efficacité et d'efficience qu'elle procure. Sur les sujets finances, achat et logistique, des conventions et protocoles interservices permettent soit une mutualisation des activités avec échange de bonnes pratiques, soit une négociation de tarifs plus avantageux, ou encore des réallocations de crédits en fonction de l'avancée des travaux respectifs.

La démarche de mutualisation engendre toutefois des coûts importants de coordination (multiplication des réunions, logistique, etc.). Cette situation génère un paradoxe : bien qu'ayant des besoins critiques sur les plans technique et capacitaire, les services les plus petits ont du mal à exploiter le plein potentiel offert par les programmes mutualisés, en raison de ressources humaines par définition limitées pour participer activement à la gouvernance de ces programmes. Tous les programmes ne peuvent par ailleurs être mutualisés à l'ensemble de la communauté du renseignement, compte tenu des différences métier substantielles et des environnements administratifs et techniques différents de chaque service.

3. Des moyens supplémentaires

Cinq milliards d'euros sont consacrés au renseignement par la LPM 2024-2030. Tous les services de renseignement ont bénéficié d'une augmentation substantielle de leurs moyens budgétaires et humains, en dépit de la crise des finances publiques que traverse notre pays. Les attentats de 2015 ont été le catalyseur de cette prise de conscience de la nécessité de réarmer notre appareil

de renseignement. L'évolution du contexte géopolitique vient confirmer cet impératif, dans le cadre de la mise en œuvre des priorités de la nouvelle *Revue nationale stratégique*.

a. La priorité budgétaire donnée au renseignement

À la DGSE, la moyenne des crédits alloués par la LPM 2019-2025 est en progression de 69 % par rapport à la LPM précédente 2014-2018. La ressource totale s'est élevée à 3,3 milliards d'euros sur la période 2019-2015. La LPM 2024-2030 prévoyait pour la DGSE une ressource en crédits de paiements à hauteur de 4,6 milliards d'euros, soit une évolution de + 53 % par rapport à la précédente loi de programmation. Dans un double contexte de réforme interne du Service et de la préparation de son déménagement vers le Fort neuf de Vincennes, ces crédits supplémentaires doivent permettre à la DGSE de conserver sa capacité à relever les grands défis techniques qui structureront son évolution dans les années à venir et qui garantiront son rôle central dans la mutualisation des capacités techniques de la communauté nationale du renseignement.

À la DGSI, le volume de crédits dépensés a plus que doublé entre 2015 et 2024. Ceci reflète la traduction budgétaire de la priorité fixée au service de sécurité intérieure en matière de lutte contre le terrorisme après les attentats de 2015. En autorisation d'engagement, le budget de la DGSI est ainsi passé de 41,6 millions d'euros en 2015 à 111,6 millions d'euros en 2024. Les crédits de paiement sont quant à eux passés de 44,7 millions d'euros en 2015 à 95,8 millions d'euros en 2025.

À la DRM, les dépenses de fonctionnement du Service ont quasiment doublé entre 2014 et 2024, passant de 24,6 millions d'euros en 2014 à 47,2 millions d'euros en 2024. Si on y ajoute les crédits d'investissements, on atteint un total de dépenses de 62,17 millions en 2024 contre 40,8 millions d'euros dix ans auparavant.

À la DRSD, la LPM 2014-2019 accordait 77 millions d'euros en crédits de paiement sur la période, essentiellement fléchés sur des dépenses de fonctionnement. La LPM 2019-2025 avait initialement porté ce montant à 120,7 millions d'euros, lequel a été fortement réévalué au cours des différents exercices d'ajustement annuel pour atteindre près de 220 millions d'euros sur la période. Ces abondements de ressources ont notamment permis d'initier le financement de projets d'investissements majeurs : SIRCID ***** et rénovation du système d'information SOPHIA *****. L'évolution la plus importante est liée au financement de la construction du nouveau siège de la direction centrale au fort de Vanves. La LPM 2024-2030, avec une ressource portée à 233 millions d'euros, consacre une nette évolution du budget de la DRSD qui est ainsi doublé entre 2014 et 2030 (hors construction du nouveau bâtiment du siège central) avec 31,4 millions d'euros en 2030 contre 16 millions d'euros en 2014.

À la DNRED, c'est la LPM 2019-2025 qui avait sensiblement augmenté les moyens du service puisque les crédits de paiement (fonctionnement et investissement) sont passés de 10,3 millions d'euros en 2019 à 27,6 millions d'euros en 2024.

À Tracfin, l'évolution des dépenses au cours de la décennie écoulée doit s'apprécier à l'aune de la croissance de la taille du service sur la période et de son besoin continu de s'adapter aux objectifs politiques réaffirmés (en matière de lutte contre la fraude ou la criminalité organisée, notamment), à la sophistication croissante des fraudes et à la hausse exponentielle du volume de déclarations de soupçons reçues par le service. L'exécution budgétaire témoigne d'un changement d'échelle *****. Pour répondre à ces enjeux, Tracfin a vu croître ses besoins de fonctionnement au travers, notamment, d'acquisition de logiciels métiers spécialisés, d'acquisition et de renouvellement de licences, de coûts liés à la refonte d'applications métier, au développement d'outils de *data science* et d'intelligence artificielle, etc. S'agissant des dépenses d'investissement, elles concernent essentiellement la sécurisation du système d'information en matière d'infrastructure (acquisition de serveurs, chiffreurs, diodes…). *****.

b. Des moyens humains supplémentaires

Tous les services de renseignement ont vu leurs effectifs augmenter significativement au cours de la décennie écoulée. Cette hausse du nombre des agents est allée de pair avec une importante diversification des profils recrutés, et une proportion plus importante des personnels civils et des contractuels par rapport aux personnels militaires et aux emplois de fonctionnaires.

À la DGSE, le nombre d'ETP ***** en 2025, soit une hausse de 29 %. Cette augmentation globale révèle des disparités importantes puisque les emplois créés dans le secteur du numérique ont progressé de 79 % quand ceux du renseignement n'ont évolué qu'à + 18 %. *****.

À la DGSI, la trajectoire est similaire. Trois plans gouvernementaux sont venus renforcer les effectifs du Service depuis sa création en 2014 *****. Le plan de renfort quinquennal 2013-2018 a alloué ***** à la DGSI, le plan de lutte antiterroriste ***** et le pacte de sécurité 2016-2017 *****. Puis entre 2017 et 2024, la DGSI a connu une hausse *****, cette progression intégrant le transfert de l'UCLAT en 2020. Le Service a ainsi réalisé ***** depuis 2018 pour atteindre ***** en 2024. L'effectif cible de 2025 qui était de ***** n'a toutefois pas été atteint du fait d'un schéma d'emploi nul notifié au cours de cette année. La DGSI développe une stratégie de *sourcing* et de recrutement spécifique aux métiers en tension *****.

La DRM est quant à elle passée de 1 640 agents en 2015 ***** à 1926 agents fin 2025 ***** dans le cadre d'une cartographie des emplois et compétences de 2 022 ETP. À l'horizon 2030, selon la prévision d'effectifs décrite dans le cadre de la LPM 2024-2030, la DRM devrait disposer de 2 286 postes.

Le service de renseignement militaire a ainsi obtenu 335 postes supplémentaires, destinés à consolider les métiers socles du renseignement *****.

À la DRSD, après avoir connu une très longue période de diminution de ses effectifs (- 23 % entre 2007 et 2014), l'année 2015 a marqué une rupture avec une remontée en puissance du Service. Depuis une dizaine d'années, la DRSD qui s'est modernisée et a connu une profonde transformation, a accru ses effectifs de plus de 55 % (+ 581 postes). Au 31 décembre 2025, la DRSD comptait 1 630 militaires et civils pour une cible fixée par la LPM 2019-2024 à 1 666, soit un taux de réalisation de 98 %. 49 créations de poste ont été accordées à la DRSD au titre de la LPM 2024-2030, ce qui devrait permettre au Service d'atteindre un effectif total de 1 701 ETP à l'horizon 2030.

Cette « réparation » s'est construite principalement avec le recrutement de personnels civils qui représentent aujourd'hui 40 % des effectifs du Service contre 23 % en 2007. Par ailleurs, les profils et la typologie du personnel ont également évolué avec, avant tout, l'augmentation de la proportion des cadres : + 55 % pour les officiers et + 93 % pour les civils de catégorie A. Même si le Service a pu bénéficier d'un accroissement significatif du nombre d'officiers, le recours aux personnels civils a été exponentiel entre 2014 et 2023 afin de pallier le manque de compétences spécifiques en personnels militaires. L'accroissement significatif des cadres et des agents de maîtrise traduit l'évolution des besoins en expertise et hautement qualifiés et marque la forte diminution du recours au personnel d'exécution : depuis 2007, on observe une baisse de 59 % du nombre de militaires du rang et de 43 % en ce qui concerne les agents de catégorie C.

Enfin, depuis 2015, les emplois en lien avec les systèmes d'information et de communication sont beaucoup plus nombreux (13 % en 2025 contre 8 % en 2014). Cet accroissement traduit la prégnance des enjeux numériques, cyber et des sciences de la donnée, qui sont au cœur de l'évolution des métiers du renseignement. Les créations de postes prévues par la LPM 2024-2030 confirment cette tendance : elles sont dédiées au cœur de métier du renseignement (à hauteur de 29) et du numérique/cyber (à hauteur de 20).

La DNRED, pour sa part, a gagné environ une centaine d'effectifs entre 2014 et 2025, passant de 726 ETP à 828 au cours de la période. *****.

À Tracfin, le plafond d'emploi du service est passé de 144 ETP en 2017 à 192 en 2023. Sur cette période, Tracfin a recruté majoritairement des enquêteurs ainsi que des experts OSINT destinés à armer le département technique du développement capacitaire, créé en septembre 2023. Pour accompagner la montée en puissance des départements métiers, Tracfin a accueilli dans ses rangs des spécialistes des métiers du numérique. Le Service a également recruté des profils techniques spécialisés qui n'existent pas dans la fonction publique (enquêteur organisme à but non lucratif, expert-comptable avocat fiscaliste, etc.). Fin 2024, les enquêteurs et analystes représentaient 50 % des effectifs de Tracfin, contre 13 % pour les agents du département informatique.

Sur la période 2023-2027, Tracfin s’est vu notifier une trajectoire de + 75 ETP notamment justifiée par la tenue des Jeux Olympiques de Paris 2024, la contribution du Service à la feuille de route du plan de lutte contre toutes les fraudes aux finances publiques et aussi la création en 2024 de l’agence européenne de lutte contre le blanchiment, laquelle exige, en application des textes européens, le recrutement et la mise à disposition d’un délégué dédié à Tracfin.

___

II. AFFIRMER LE RENSEIGNEMENT COMME GARANT DE NOTRE AUTONOMIE D'APPRÉCIATION, CONDITION D'EXERCICE DE NOTRE SOUVERAINETÉ

Dans un monde où l'influence s'exerce autant par la donnée que par la force, disposer de ses propres capacités de renseignement n'est plus un avantage : c'est bel et bien une exigence fondamentale de souveraineté.

Un appareil de renseignement fournissant une analyse indépendante et fiable constitue un pilier essentiel de l'autonomie d'appréciation des autorités. Sans cette maîtrise souveraine de l'information, toute décision politique, diplomatique ou militaire s'expose au risque de la dépendance et de l'erreur d'appréciation. Affirmer le rôle central du renseignement équivaut ainsi à garantir la liberté de jugement des autorités, condition nécessaire à l'exercice d'une souveraineté réelle et non simplement proclamée.

Les prérequis d'un renseignement doté de capacités autonomes sont multiples et concernent :

– Un investissement continu, tant humain que technologique.

– Une base industrielle et technologique souveraine en mesure de fournir les capacités techniques clefs, tant dans le domaine de la collecte que du traitement des données.

– Des acteurs nationaux dans les infrastructures numériques en mesure d'assurer l'effectivité de la mise en œuvre des techniques de renseignement.

– Une protection du secret entourant les sources, méthodes et capacités utilisées et développées.

– Un cadre juridique adapté.

– Une politique maîtrisée de coopération.

A. VISER L'AUTONOMIE DANS L'INTERDÉPENDANCE

Aux termes de la *Revue nationale stratégique*, dans sa version classifiée : *****.

1. Maîtriser nos alliances

Éviter la dépendance sans pour autant renoncer aux alliances : dans le domaine du renseignement, l'autarcie n'est ni souhaitable, ni réaliste. Il s'agit pour les services de viser l'autonomie dans l'interdépendance, en conservant la maîtrise de leurs partenariats.

Un sujet pour les services de renseignement du monde entier est celui de leur dépendance plus ou moins forte aux capacités américaines. On se souvient de l'enjeu stratégique qu'il y avait pour la France, en 2003, à disposer de capacités souveraines d'observation dans le dossier irakien autour des armes de destruction massive. Cette maîtrise du renseignement est centrale dans la définition d'une position politique souveraine et donc libre.

Pour autant, la coopération de nos services avec des partenaires étrangers demeure essentielle. À cet égard, tant le directeur général de la sécurité extérieure (DGSE) que le coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT) ont affirmé, lors de leurs auditions par la DPR, que l'arrivée au pouvoir de l'administration Trump ne se traduisait pas, à ce stade, par une rupture dans la coopération entre les services français et leurs homologues américains, en particulier dans le domaine de la lutte contre le terrorisme.

La coopération transatlantique concerne de nombreux autres domaines. *****.

Un renseignement autonome repose sur l'investissement et le développement de capacités de recueil, condition essentielle pour éviter d'engager des partenariats ***** avec des services étrangers pour bénéficier de leurs capacités techniques. *****.

Les changements géopolitiques ont progressivement redessiné la cartographie des partenariats des services français. Mais les logiques propres aux coopérations en matière de renseignement ne recouvrent pas entièrement les logiques diplomatiques. En matière de lutte anti-terroriste, le partage de renseignements ou d'analyse sur la menace demeure ainsi la règle, indépendamment de l'environnement politique ou géopolitique.

Le monde du renseignement se révèle extrêmement agile en termes de coopération, avec une capacité à nouer de nouvelles coopérations ou d'en suspendre dans un temps relativement bref. La recomposition du dispositif français en Afrique a ainsi redessiné la carte des partenariats de la DRSD, *****.

L'orientation donnée aux échanges de renseignement et d'analyse est ainsi très fortement corrélée à l'évolution géopolitique. Si le renforcement des coopérations a notamment été marqué au cours des vingt dernières années en matière de contre-terrorisme, la période actuelle est marquée par le renforcement des échanges dans le domaine du contre-espionnage et de la contre-ingérence. Ces échanges portent à la fois sur la perception de la menace et sur la mise en œuvre des mesures défensives communes (politique de vigilance consulaire, mise en œuvre simultanée d'entraves opérationnelles dans plusieurs pays européens, dénonciation coordonnée d'activité d'ingérence et d'espionnage). **Le déclenchement de la guerre en Ukraine a entraîné une hausse nette des échanges sur la Russie**. *****. De manière générale, la réaffirmation des « États puissance » s'accompagne

d’un renforcement des collaborations dans le domaine du contre-espionnage russe, ***** et iranien.

*****.

Le renforcement de la présence otanienne sur le flanc Est s’est pour sa part accompagné d’une montée en puissance de la contre-ingérence au sein de l’Alliance atlantique. C’est ainsi que la DRSD s’intègre, en tant que service national de contre-ingérence Défense, aux efforts portés par l’OTAN dans ce domaine par une participation systématique régulière aux exercices interalliés, aux séminaires spécialisés et aux travaux de révision des doctrines conjointes de contre-ingérence. *****.

Si le partenaire américain demeure incontournable, une dynamique profonde de rapprochement entre services de renseignement est à l’œuvre et la DGSE joue un rôle de premier plan dans la montée en puissance de l’autonomie stratégique européenne. La DRM veille pour sa part à l’identification des partenaires qui seront potentiellement utiles à long terme, dans une approche délibérément transactionnelle. Dans ce cadre, les postures affichées au sein des instances multilatérales (UE, OTAN, forums de renseignement ad hoc), mais aussi l’évaluation des accès réels des partenaires, sont à prendre en compte.

C’est au regard de cette bascule d’effort du renseignement vers le flanc Est de l’Europe que la délégation a décidé d’effectuer une mission spécifique aux pays limitrophes des frontières russe et biélorusse.

Déplacement à Varsovie et à Riga du 12 au 14 novembre 2025

Une délégation composée de Mmes Agnès Canayer, Caroline Colombier et Gisèle Jourda, s'est rendue à Varsovie et Riga, du 12 au 14 novembre 2025, sur la thématique du rapport 2025 : le renseignement français face au désordre mondial. La mission comportait un double objectif, d'abord celui des enjeux de sécurité et de renseignement dans la région, propres aux compétences de la DPR (menaces géopolitiques, finalités du renseignement, moyens, coopérations, etc.), ensuite celui de la vérification des fonds spéciaux employés par les postes concernés.

Ces deux pays, Pologne et Lettonie, ont été choisis pour trois séries de motifs :

– leur situation géographique, respectivement à la frontière de l'Ukraine, de la Biélorussie et de la Russie ;

– leur exposition aux tensions politiques et aux menaces issues, conventionnelle ou hybrides, de la guerre en Ukraine ou des ingérences étrangères attribuées au voisinage biélorusse et russe ;

– et le renforcement récent du dispositif français, notamment en matière de renseignement, en Pologne comme dans les pays baltes.

Le programme comportait ainsi trois dimensions avec en premier lieu des entretiens avec les ambassadeurs de France – respectivement MM. Étienne de Poncins et Manuel Lafon Rapnouil, ***** – intégrant pour ces derniers un volet de contrôle sur place et sur pièce au titre de la CVFS, puis des rencontres avec les autorités locales (en Pologne avec M. Kazimierz Plocke, président de la commission des services spéciaux de la Diète, l'Agence de renseignements extérieurs « Agencja Wywiadu » (AW) et en Lettonie avec les présidents des commissions de la sécurité nationale et de la défense), enfin un échange de vues avec Mme Katarzyna Pisarska, présidente, et des membres de la fondation Casimir Pułaski (think tank polonais qui organise le forum annuel de sécurité de Varsovie) à l'occasion de la parution d'un rapport sur la guerre cognitive et les actions clandestines menées par les services secrets russes et biélorusses (*« Agents of Chaos: the Shadow Campaign Against the West – Cognitive Warfare and Covert Action by Russian and Belarussian Intelligences Services » – Fondation Casimir Pulaski- 2025*).

Il est notable que les services de renseignement aient souhaité rencontrer la délégation, signe de l'intérêt porté à cette mission.

Deux séries de constats et d'enseignement ont pu être dressées au cours de cette visite.

Au chapitre des constats, l'état des lieux dressé par les interlocuteurs contraste avec la perception de la menace et des besoins qui peut être faite depuis l'hexagone. En Pologne comme en Estonie, par l'usage du terme de « menace hybride », il est moins question de menaces potentielles que d'actions hostiles très concrètes et matérielles telles que :

– des ingérences numériques prenant la forme de manipulation de l'information ayant pour but de diviser la population (par exemple entre la communauté russophone et les autres Lettons) ou d'attaques cyber visant à désorganiser des infrastructures énergétiques et de transport ;

– des sabotages sur des lignes et des ponts ferroviaires, ainsi que des incendies volontaires, notamment dans un centre commercial en Pologne ;

– des survols de drones en Lettonie et en Pologne, celle-ci ayant fait face en septembre 2025 à l'incursion d'une vingtaine de drones russes, qu'elle considère comme étant une manœuvre volontaire et dont 4 d'entre eux ont été abattus par les forces aériennes polonaises et néerlandaises dans le cadre de la mission de protection de l'espace aérien de l'OTAN ;

– enfin, des franchissements de migrants des frontières polonaise et lettone en contact avec le territoire biélorusse dont l'organisation est attribuée à la Biélorussie. Les interlocuteurs polonais et lettons rattachent ce phénomène à celui de la guerre hybride plutôt à une problématique police des frontières. L'interprétation qui a pu en être donnée est celle d'une utilisation politique de ce phénomène afin d'obtenir un soutien financier de l'Union européenne pour sécuriser les frontières.

Il ressort également que les services de renseignement polonais et letton, qui se focalisent essentiellement sur la menace russe, disposent donc d'une expertise très utile mais de fait assez restreinte. Ce qui les ouvre naturellement et de manière spontanée à un partenariat avec les services français dont le spectre de compétence est plus large. *****.

En contrepoint des contraintes d'effectifs et d'implantation immobilière, il est apparu à la délégation que l'ensemble des interlocuteurs accordait une confiance et un intérêt tout particulier au développement du partenariat avec le renseignement français dans la mesure où il demeure le seul pays pouvant apporter une analyse autonome de l'allié américain, tant dans le renseignement d'ordre tactique sur le théâtre ukrainien que stratégique. Ceci confère à la France une responsabilité particulière dans la permanence de ses capacités de détection et d'analyse souveraine. Réciproquement, la collaboration avec les partenaires polonais et baltes apporte à la France une expertise linguistique et analytique plus ciblée sur la Russie et la Biélorussie.

2. Limiter nos dépendances

Alors que l'innovation technologique évolue à un rythme soutenu, le renseignement français ne peut faire l'impasse sur des outils étrangers lorsque ceux-ci apportent une valeur ajoutée incontestable, mais à condition d'en maîtriser les risques associés. Les services de renseignement ont ainsi fréquemment recours à des technologies étrangères, ce qui ne pose pas en soi de difficulté dès lors que cela ne crée pas de situations de dépendances potentiellement critiques.

Or cela peut être le cas quand des systèmes d'information sont bâtis exclusivement sur des solutions étrangères. Si la DRSD considère *****.

Tracfin a également recours à des solutions techniques étrangères pour le suivi des transactions en cryptoactifs. *****. Certaines recherches peuvent certes être effectuées en utilisant des informations en sources ouvertes mais les solutions américaines offrent un accès aux données liées aux transactions en cryptoactifs (notamment en termes de localisation) dont Tracfin ne peut aujourd'hui se passer. *****.

3. Agir dans le cadre d’un État de droit

Les services français de renseignement inscrivent leur action dans le cadre strict de l’État de droit, conformément aux lois et règlements qui encadrent leurs missions et aux contrôles démocratiques auxquels ils sont soumis. Cette exigence repose sur un équilibre permanent entre efficacité opérationnelle et respect des libertés fondamentales. Force est de constater qu’elle crée aussi une asymétrie juridique avec les services de renseignement d’États non démocratiques, dont les pratiques peuvent être dénuées de tout contrôle ou de garanties pour les citoyens.

Nos services sont confrontés à une difficulté liée au **décalage entre le temps du droit et le temps de l’opérationnel**.

Le sujet du chiffrement illustre cet état de fait. Depuis que les communications se sont massivement numérisées, la cryptographie n’est plus l’apanage des ingénieurs ou des institutions financières ; elle est devenue le langage quotidien de milliards d’échanges, des plus anodins aux plus sensibles. Cet usage généralisé, prolongement naturel de la quête de confidentialité des citoyens et des entreprises, redéfinit continuellement les frontières de l’action publique.

Pour les services de renseignement, cet environnement représente un double paradoxe. D’un côté, le chiffrement constitue un rempart indispensable contre l’espionnage étranger, la cybercriminalité et les intrusions qui menacent les infrastructures vitales. Il est l’allié naturel de la souveraineté numérique. De l’autre, il complique l’accès légal à des informations cruciales lorsque des groupes hostiles, criminels ou terroristes en détournent l’usage pour échapper à toute détection. Le défi n’est donc pas le chiffrement en lui-même, mais l’impossibilité d’articuler pleinement sécurité collective et confidentialité absolue dans un espace numérique devenu opaque.

Le cadre légal français, issu des lois de 2015 et 2021, s’efforce de répondre à cette tension en conciliant efficacité opérationnelle et exigences démocratiques. Or dans l’état actuel du droit, les plateformes de messageries chiffrées peuvent arguer d’arguments techniques pour ne pas répondre aux demandes d’accès des autorités. En effet, l’article L. 871-1 du code de la sécurité intérieure (CSI) prévoit pour seule obligation pour les « prestataires de cryptologie » de fournir les clefs de déchiffrement. Or ces acteurs ne les détiennent pas. Les grandes plateformes ont effet érigé depuis l’affaire *Snowden* la protection des échanges induite par la non-détention de ces clefs comme un argument commercial majeur. Au-delà de ces arguments techniques, ces mêmes acteurs tendent à ne pas répondre aux réquisitions adressées par les autorités françaises dans un cadre de renseignement sur des demandes d’identification de numéros ou de dates d’appels, qui ne sont pourtant pas chiffrées. Certains opérateurs établis à l’étranger réfutent l’application de la loi française. En l’absence de sanctions crédibles, ces opérateurs ne coopèrent pas avec les services de renseignement.

Dans ce contexte, **une part croissante des communications échappe à toute possibilité de surveillance,** en dépit des prérogatives larges accordées par le législateur aux services de renseignement. Cette tendance va s'accentuer avec la généralisation des mécanismes de chiffrement dans les produits grand public, le chiffrement généralisé des SMS à très court terme et des conversations téléphoniques à moyen terme. Ainsi, sans évolution normative, les services sont condamnés à se voir privés d'accès à l'essentiel des communications. Cette érosion des capteurs techniques des services intervient alors que la menace se situe à un niveau exceptionnellement élevé.

À l'échelle européenne, cette exigence démocratique prend une dimension supplémentaire avec la double jurisprudence de la Cour de justice de l'Union européenne (CJUE) et de la Cour européenne des droits de l'homme (CEDH) qui affectent l'activité des services de renseignement.

Le juge européen a, au terme d'une jurisprudence bien établie [(1)], livré son interprétation de l'article 4.2 du Traité sur l'Union européenne, en vertu duquel la sécurité nationale relève de la seule responsabilité des États membres, en considérant que « *bien qu'il appartient aux États membres de définir leurs intérêts essentiels de sécurité et d'arrêter les mesures propres à assurer leur sécurité intérieure et extérieure, le seul fait qu'une mesure nationale a été prise aux fins de la protection de la sécurité nationale ne saurait entraîner l'inapplicabilité du droit de l'Union et dispenser les États membres du respect nécessaire de ce droit* ».

Cette interprétation emporte des conséquences opérationnelles pour les services de renseignement, s'agissant en particulier des règles de conservation des données. Par ses arrêts *Tele 2 Sverige* AB du 21 décembre 2016 et *La Quadrature du Net* du 6 octobre 2020, la Cour de justice de Luxembourg prohibe en effet toute législation nationale autorisant une conservation généralisée et indifférenciée des données de connexion, à moins de justifier l'existence d'une menace réelle, actuelle et prévisible pour la sécurité nationale.

Cette jurisprudence irrigue désormais l'ensemble des arrêts de la Cour, en témoigne l'arrêt ligue des droits humains du 21 juin 2022 s'agissant des données PNR. Le juge de Luxembourg valide la directive PNR, en l'encadrant toutefois de manière très stricte en considérant que l'application de la directive doit être limitée à la lutte contre les infractions terroristes et les formes graves de criminalité. Ce raisonnement pourrait conduire notamment à exclure l'utilisation du système PNR pour d'autres finalités que celles expressément prévues par la directive, comme la préservation des intérêts fondamentaux de la Nation prévue à l'article L. 232-7 CSI *****.

(1) CJUE, 4 juin 2013, ZZ point 38 ; CJUE, 20 mars 2018, Commission / Autriche, points 75 et 76 ; CJUE, 2 avril 2020, Commission / Pologne, Hongrie et République tchèque, points 143 et 170 ; CJUE, 6 octobre 2020, La Quadrature du Net, point 99.

Par ailleurs, la jurisprudence de la CEDH (Cour européenne des droits de l'Homme) peut également avoir des impacts sur les activités des services. Par son arrêt *Podchasov c. Russie* du 13 février 2024, le juge de Strasbourg s'est en effet récemment opposé à toute pratique conduisant à un affaiblissement du chiffrement.

Ces jurisprudences européennes peuvent apparaître comme déconnectées des réalités techniques et opérationnelles et font peser un risque majeur sur la capacité des services de renseignement à conduire leurs investigations.

Se pose enfin la question récurrente des échanges de renseignement avec des services étrangers pour lequel il existe dans notre pays un vide juridique qui pourrait conduire à une condamnation de la France, faute d'encadrement suffisant en la matière. La DPR réitère sa préconisation d'un dispositif inspiré des règles en vigueur au Royaume-Uni.

B. ÉVITER LE DÉCROCHAGE

Dans un contexte international marqué par l'accélération des ruptures technologiques et la compétition stratégique entre puissances, le renseignement français doit se mettre en situation d'éviter tout décrochage.

L'émergence de capacités fondées sur l'intelligence artificielle, le quantique ou les technologies spatiales redéfinit en profondeur les équilibres sécuritaires, plaçant les services face à des adversaires toujours plus agiles et mieux équipés. Pour rester dans la course, la France doit investir résolument dans des programmes souverains capables de garantir son autonomie technologique et informationnelle. Cet effort passe aussi par une politique ambitieuse d'attractivité des métiers du renseignement, condition indispensable pour recruter et fidéliser les expertises rares nécessaires à la puissance publique. Enfin, l'adaptation du cadre juridique, afin d'éviter que certaines contraintes obsolètes ne freinent l'efficacité opérationnelle, constitue un autre levier essentiel pour permettre aux services de remplir pleinement leurs missions. Préserver la performance du renseignement français rend ainsi nécessaire de conjuguer innovation, souveraineté, ressources humaines et modernisation normative.

1. Anticiper les ruptures technologiques

a. L'intelligence artificielle

Le principal risque à court et moyen terme en matière de décalage technologique réside dans l'intelligence artificielle. La maîtrise de cette technologie de rupture et sa démocratisation dans les domaines du renseignement technique, depuis l'acquisition des données jusqu'à leur exploitation, constituent un enjeu immédiat et crucial, susceptible soit d'offrir un avantage stratégique, soit d'exposer la communauté du renseignement à un risque de décrochage.

Le secteur privé dispose aujourd'hui d'un afflux de capitaux sans commune mesure avec ce que le secteur public est en capacité de faire. Les principaux LLM sont américains avec peu d'alternatives, dans le domaine des GPU (calculateurs) qui deviennent des biens stratégiques susceptibles de se voir placés sous embargo total ou partiel.

Cela impacte tout à la fois la capacité à transcrire et traduire des contenus, mais aussi à produire des synthèses et des analyses et à procéder à des recherches dans les jeux de données massives recueillies ou en source ouverte sur le web (Osint).

*****. L'enjeu recouvre à la fois la capacité à produire les modèles et à les mettre en œuvre sur le matériel nécessaire.

b. La technologie quantique

*****. Le potentiel que représente la technologie quantique apparaît comme un instrument de puissance stratégique pour qui saura la maîtriser. Trois domaines d'application du quantique intéressent particulièrement le renseignement militaire : les capteurs et la métrologie, l'informatique et enfin les communications. La menace de nos compétiteurs disposant de ces capacités ne peut être négligée.

La révolution quantique place les services de renseignement face à un horizon à la fois prometteur et inquiétant. D'un côté, ces technologies offriront la possibilité de communiquer à l'abri de toute interception grâce à des échanges de clés impossibles à espionner, de détecter des menaces invisibles ou de décrypter des masses d'informations avec une rapidité inédite. De l'autre, elles vont fragiliser les fondations mêmes du secret : un ordinateur quantique suffisamment puissant pourrait briser les protections cryptographiques qui sécurisent aujourd'hui les communications diplomatiques, militaires ou gouvernementales. Ainsi, le quantique est à la fois un bouclier et une brèche, un atout qui pourrait renforcer les capacités d'analyse et de surveillance – mais aussi une menace qui rend obsolètes les défenses d'hier. Pour les services de renseignement, il s'agit de ne pas se laisser dépasser par une technologie qui rebat les cartes du pouvoir et du secret.

c. L'avenir du secteur spatial

Les ruptures technologiques dans le domaine spatial redessinent profondément le paysage du renseignement, en multipliant à la fois les outils d'observation et les zones d'incertitude. La miniaturisation des satellites, leur production industrielle et l'explosion des constellations en orbite permettent désormais une couverture quasi continue de la Terre, offrant aux services de renseignement une vision plus fine, plus fréquente et plus réactive des crises émergentes. Les avancées en propulsion, en robotique orbitale ou en détection hyper-spectrale ouvrent la voie à une surveillance plus discrète et plus précise, capable de dévoiler des activités autrefois invisibles.

Mais ces opportunités s'accompagnent de risques inédits. La congestion de l'orbite, la multiplication d'acteurs privés aux capacités parfois équivalentes à celles des États, et l'apparition de technologies antisatellites fragilisent un domaine devenu essentiel à la sécurité nationale. **À mesure que l'espace se militarise et se privatise, le renseignement perd son monopole sur l'observation et doit composer avec un environnement où les images, les données et les trajectoires sont potentiellement accessibles à tous.** Dans ce nouvel écosystème, les services doivent réinventer leur supériorité technologique, faute de quoi ils pourraient se retrouver dépendants d'infrastructures vulnérables ou dépassés par des adversaires capables de voir – ou de rendre invisibles – bien plus vite qu'eux. *****.

2. Investir dans des capacités souveraines

« *Les services renforceront la mutualisation de leurs moyens techniques, à la faveur de nouveaux investissements et de développements capacitaires. Les services de renseignement exploiteront tout le potentiel des technologies de rupture, en déclinant les stratégies en matière d'intelligence artificielle et de technologies quantiques de l'État. L'expertise technique de pointe souveraine en matière de détection, recueil, décryptement, traitement et analyse de l'information, y compris sur son volet spatial, sera également renforcée. Par ailleurs, ils devront soutenir les filières technologiques industrielles souveraines, dans les domaines capacitaires où l'autonomie stratégique et la résilience sont primordiales* ».

Revue nationale stratégique 2025

La communauté du renseignement se met en ordre de marche pour développer des capacités souveraines dans les champs stratégiques identifiés par la nouvelle *Revue nationale stratégique*. Plusieurs projets de mutualisation dans le domaine technique répondent aux objectifs fixés par la RNS.

a. Sécuriser les systèmes d'information

La vulnérabilité des systèmes d'information des services d'information impose de les sécuriser. À cette fin, la DGSI conduit deux projets majeurs :

– Le premier est celui du *datacenter* du ministère de l'Intérieur qui permettra de doter la DGSI et les services du second cercle rattachés au ministère (renseignement territorial, DRPP) d'un centre de données à l'état de l'art, tout particulièrement pour les aspects de sécurité des systèmes d'information (SSI).

– Le second est le projet de site unique, qui comporte un volet « centre de données » garantissant à la DGSI une complète résilience au travers d'un site miroir informatique.

Le projet d'interconnexion des réseaux classifiés des services du 1er et du 2e cercle est également un projet capacitaire structurant. Il offrira un espace d'échange et de communication commun de niveau « Secret », garantissant un plus haut niveau

de sécurisation et une plus grande fluidité aux dix services de renseignement, à la CNCTR, la CNRLT, la DGA et le GIC.

b. Développer des programmes capacitaires structurants

*****. La DGSI a aussi lancé, dès 2021, un vaste **programme interministériel de conception et de réalisation d'un outil de traitement de données hétérogènes**, pour notamment remplacer celui de la société américaine *Palantir*. Le projet, dénommé OTDH, concerne sept des dix services de renseignement, des directions de la DGPN et de la DGGN, mais aussi de la DFGFIP et de la DGDDI. *****. Cette capacité souveraine, qui a vocation à être partagée par l'ensemble des services de renseignement, pourrait répondre à de multiples besoins sur le périmètre de l'exploitation et l'analyse de données. Les outils ont vocation à devenir une alternative française crédible à des produits étrangers, aucune entreprise française n'étant à l'heure actuelle aux standards du marché sur la plupart de ces périmètres. *****.

En matière de contre-ingérence informationnelle, la DRSD est engagée *****. Alors que les manœuvres hostiles de ce type tendent à se multiplier pour exploiter la forte résonance médiatique offerte par le cyberespace, la DRSD travaille en partenariat avec les services du premier cercle et d'autres partenaires ministériels et interministériels.

Pour sa part, la DRM veille à conserver, dans chaque domaine, une capacité souveraine socle. Les principaux investissements prévus pour garantir la souveraineté technologique du service de renseignement militaire concernent le segment spatial optique et électromagnétique. Les grands groupes industriels tels qu'Airbus et Thalès sont les pourvoyeurs de ces capacités souveraines. En outre, les capacités dans la très haute altitude (drones, ballons, dirigeables) doivent être expérimentées afin de définir la pertinence de ce type de vecteurs pour le renseignement. Dans le domaine du REOM, de nouvelles capacités souveraines pourraient voir le jour, s'agissant de la très haute altitude, avant 2030. En revanche, s'agissant de l'imagerie Radar, la France dépend de ses partenaires et de ses capacités commerciales. *****.

Dans le domaine ***** des cryptomonnaies, *****.

c. Combler le retard en matière d'OSINT

Parce qu'une grande partie de l'information utile au renseignement est désormais publique, dispersée sur le web, et produite en quantités massives, l'OSINT est incontournable. Cela exige des compétences en collecte, en vérification et en analyse, et souvent des outils spécialisés pour gérer des volumes de données massifs. *****.

3. Renforcer l’attractivité des métiers du renseignement

Le volet humain est tout aussi important que le volet technique. Le recrutement et la fidélisation sont des enjeux fondamentaux pour les services de renseignement, quelle que soit leur taille.

Or la communauté du renseignement est confrontée à de réelles difficultés en matière de recrutement, dans un contexte fortement concurrentiel où les salaires du secteur privé sont généralement bien supérieurs. **La quasi-absence de recours au télétravail** dans la plupart des services de renseignement se révèle aussi être un handicap au recrutement.

Certains services – notamment ceux rattachés au ministère des armées – sont également confrontés à la **complexité des différents statuts et règles de gestion entre militaires et civils d’une part, mais aussi entre les armées elles-mêmes, ou entre fonctionnaires et agents sous contrat**. Cela est aussi vrai à Bercy où Tracfin emploie des agents issus d’une vingtaine de corps différents avec des interlocuteurs, des gestions RH et des régimes indemnitaires eux aussi différenciés. **La procédure d’habilitation allonge aussi considérablement les délais d’embauche** et l’équilibre entre personnels statutaires et contractuels est difficile à maintenir au vu des compétences recherchées.

Ces dernières années, **plusieurs services ont ainsi dû faire face à d’importants départs.** C’est le cas à la DGSE qui a subi une vague de démissions sans précédent en 2021 et 2022 dans le contexte post-COVID. La DGSI fait elle aussi face à un nombre de départs externes important ***** amenuisant l’effort notable de recrutement ***** et la capacité du service de renseignement intérieur à atteindre ses cibles. Face aux mutations de la société, qui bousculent la logique traditionnelle de carrière dans un même secteur d’activité, **les services ont du mal à fidéliser leurs contractuels**. *****.

Pour autant, la situation n’est pas uniforme d’un service à l’autre. Depuis deux ans, la **DRM observe *a contrario* une attractivité croissante**, avec une augmentation significative du nombre de candidatures. Pour les agents contractuels, elles sont passées de 3 000 en 2023 à 6 600 en 2025, soit une augmentation de 120 %. Parallèlement, le taux de départs a chuté *****.

Les différents services de renseignement s’emploient à développer leur **« marque employeur »**, auprès des grandes écoles et des universités et par une présence dans les salons étudiants, forums et *job dating*. Il s’agit d’accroître l’attractivité de la communauté du renseignement auprès des jeunes publics, en particulier la « génération Z » qui se distingue par des aspirations et des pratiques professionnelles nouvelles. Un *sourcing* ciblé permet d’identifier les profils à haute valeur ajoutée.

La DGSI a ainsi organisé en 2024 une journée « portes ouvertes » sur son site de Levallois-Perret pour faire connaître la diversité des métiers qu’elle propose. La DRSD a conclu des accords ***** ; ceci a permis en 2024 de recruter 23 agents

de catégorie B. **Le creuset de l'apprentissage est aussi exploité, avec des résultats très satisfaisants** puisque 26 % de 15 apprentis ont poursuivi leur carrière au sein du Service, alors que la moyenne ministérielle se situe plutôt autour de 10 %.

Pour la communauté du renseignement, **l'enjeu de la fidélisation**, *via* notamment la qualité managériale, l'amélioration des conditions de travail ou le levier financier, est tout aussi important que la capacité à recruter.

Le **levier indemnitaire** est ainsi activé à travers la mise en place de primes valorisant les contraintes réelles et croissantes liées à l'appartenance à un service de renseignement. Car ce n'est pas toujours le cas. Tracfin, par exemple, emploie 50 % de contractuels dont la rémunération et la gestion obéissent à des règles interministérielles qui ne tiennent pas compte, par principe, des spécificités du Service. *****.

Alors que la DGSE a instauré une **« prime de contrainte »** liée au respect du secret (habilitation, entretien psychologique, absence de télétravail, obligation de discrétion), *****. Dans le cadre de sa stratégie RH mise en œuvre pour renforcer son attractivité, fidéliser ses agents et accompagne sa montée en puissance, le service du renseignement intérieur a d'ores et déjà instauré une revalorisation annuelle au profit des agents exerçant l'un des 30 métiers en tension de la Direction générale. Alors que 50 % des agents contractuels exerçant un métier en tension ont moins de trois ans d'ancienneté, cette politique de revalorisation constitue un vecteur essentiel pour réduire le nombre de départs annuels et conforter les capacités souveraines de la direction.

Pour les agents contractuels relevant des métiers « renseignement et sécurité des systèmes informatiques », la DRM et la DRSD ont instauré un barème de rémunération dérogatoire depuis janvier 2018. Cette mesure comprend notamment une majorité de l'indice majoré (IM) au recrutement pour les analystes juniors, avec la possibilité d'accéder au barème d'analyste senior après trois à six ans de service. À la DRM, une indemnité temporaire de mobilité (ITM) est également mise en place pour promouvoir les postes difficiles à honorer. Ces dispositions produisent des résultats tangibles en matière de fidélisation, comme en témoigne la réduction significative du nombre de démissions à la DRM *****.

Les **écarts en matière de rémunération** sont un paramètre non négligeable à prendre en compte. Au sein du ministère des Armées, certains agents de catégorie A / *****. Aussi, dans la continuité des recommandations émises par la Cour des comptes en 2024, **il est souhaitable d'homogénéiser autant que possible le régime indemnitaire des personnels qui y servent**. C'est là un élément essentiel pour favoriser une dynamique de parcours croisés entre les services, chose difficile tant les statuts et règles de gestion diffèrent.

À cet égard, l'application du référentiel dit « DINUM 2 » pour fixer la rémunération des contractuels de la filière numérique à leur recrutement, mais aussi pour leur renouvellement ou leur revalorisation en cours de contrat, est une avancée

certaine. Il en est de même de l'application du référentiel de rémunération arrêté par la CNRLT pour les agents exerçant un métier de renseignement technique.

Au-delà du sujet lié à la rémunération, les services mènent aussi une réflexion quant à **l'évolution des modalités d'organisation du travail**. La DGSI explore ainsi différentes pistes telles qu'un élargissement de l'accès aux horaires variables dans les services opérationnels dont les régimes horaires sont prévisibles, l'aménagement de la durée hebdomadaire du travail ou encore l'expérimentation d'un dispositif de télétravail. La DGSE actionne pour sa part différents leviers tels que l'élaboration de schémas de carrières longues ainsi que l'accompagnement des personnels (services aux agents, accompagnement des conjoints lors des mobilités, plans de mobilité extérieure, télétravail…).

4. Lever des freins juridiques

Sans se prononcer sur la totalité des demandes qui suivent, portées par les services de renseignement, la Délégation estime que les évolutions législatives envisagées nécessiteraient de leur part un travail préparatoire documenté, précis et confiant avec les parlementaires pour leur exposer, sans contrevenir au secret de la défense nationale, leurs besoins opérationnels.

a. Faciliter l'accès aux communications chiffrées

Il s'agit du sujet de préoccupation majeur des services de renseignement alors que le Sénat a adopté en 1re lecture du projet de loi relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité un article 16 *bis* interdisant d'imposer aux fournisseurs de services de chiffrement, y compris aux prestataires de services de confiance qualifiés, l'intégration de dispositifs techniques visant à affaiblir volontairement la sécurité des systèmes d'information et des communications électroniques tels que des clés de déchiffrement maîtresses ou tout autre mécanisme ou processus permettant un accès non consenti aux données protégées.

Si la cryptographie est une technologie indispensable à la sécurité numérique, avec des usages multiples, la généralisation de son utilisation entrave de plus en plus les enquêtes administratives et judiciaires. Le constat unanimement partagé est celui d'un amoindrissement des accès aux contenus « en clair » puisque les messageries chiffrées se substituent aux moyens de communication traditionnels (SMS, téléphonie).

Il existe deux types de réponses à cette situation :

– soit contraindre les opérateurs à fournir eux-mêmes un accès aux données claires dont l'interception aurait été légalement autorisée même si la domiciliation à l'étranger de la grande majorité d'entre eux en fragilise l'application ;

– soit permettre à l'autorité judiciaire et aux services de renseignement de capter les données à la source, avant leur chiffrement. *****.

Malgré la fin de non-recevoir qui lui est jusqu'à présent opposée, la communauté du renseignement reste en demande d'une évolution législative pour rééquilibrer le rapport de force avec les opérateurs et obtenir un accès aux communications chiffrées, en prévoyant explicitement qu'elle s'applique aux opérateurs domiciliés hors du territoire national.

La Délégation estime nécessaire de faire évoluer le droit pour tenir compte des évolutions technologiques et de la perspective, à court terme, d'une généralisation du chiffrement de l'ensemble des communications rendant *de facto* inopérants les mécanismes actuels d'interception.

L'autorisation d'accéder aux communications chiffrées devrait bien entendu s'accompagner de garanties juridiques et techniques solides pour répondre aux inquiétudes des acteurs du secteur qui font valoir que tout accès, même ciblé, à des données chiffrées fragiliserait le chiffrement dans son ensemble, en ouvrant des failles exploitables par des acteurs malveillants.

b. Faire évoluer à la marge le cadre légal relatif aux techniques de recueil du renseignement

Si le cadre posé par le législateur en 2015 conserve toute sa pertinence, l'évolution de la menace et les mutations technologiques rendent nécessaire d'envisager plusieurs évolutions du régime juridique de la collecte du renseignement. Plusieurs mesures de modernisation ou d'ajustement, relatives au cadre d'emploi des techniques de renseignement et aux modalités d'exploitation et de conservation des données qui en sont issues, font consensus au sein des services de renseignement. Cela concerne :

– La possibilité **d'intégration des URL dans la technique dite de l'algorithme**. Dans sa décision du 12 juin 2025, le Conseil constitutionnel a censuré l'article L. 851-3 du CSI et l'extension du champ des traitements algorithmiques aux URL, qui avait été actée par le législateur en 2021. Cette censure affecte la capacité des services à répondre à l'évolution de la menace : la perte de vitesse des moyens de communication classiques au profit d'applications de communications sur internet réduit en effet drastiquement l'efficacité des algorithmes actuels.

– La **simplification de la technique de l'algorithme** : actuellement, toute détection (« hit ») dans le cadre d'un algorithme est soumise, avant d'être communiquée au service compétent, à une procédure de désanonymisation impliquant une nouvelle décision du Premier ministre, délivrée après avis de la CNCTR. Cette procédure allonge considérablement le temps de traitement des « hits », sans apporter de garanties particulières en termes de protection de la vie privée. Cette procédure d'anonymisation pourrait être remplacée par une information en temps réel de la CNCTR sur le nombre de « hits » remontés par les algorithmes.

– **L'allongement de la durée de conservation des données brutes** issues de la technique de recueil de données informatiques. Actuellement fixée à 120 jours, elle se révèle parfois insuffisante pour l'exploitation de volumes souvent très importants de données complexes.

– *****.

– **L'extension des finalités autorisant la mise en œuvre de la technique de recueil de données de connexion en temps réel**, actuellement limitée à la prévention du terrorisme. Cette technique pourrait être étendue *****.

– **L'extension de la possibilité de s'introduire dans un lieu privé pour la mise en œuvre de la technique de recueil de données par dispositif de proximité (IMSI-catching)** : *****.

– L'extension de l'exploitation, dans le cadre de la **surveillance internationale**, des communications de personnes utilisant des identifiants rattachables au territoire national, à la sécurité économique et à la prévention des violences collectives. Les menaces suivies au titre de ces finalités présentent en effet un caractère transnational et la mise en œuvre de cette technique serait particulièrement utile pour renforcer les capacités de suivi des déplacements d'objectifs évoluant dans un environnement international.

– **La prolongation du délai de quatre mois en vigueur pour l'exploitation des données collectées dans le cadre de la surveillance d'une communication internationale**, au regard du temps long dans lequel se déploient généralement ces procédures.

c. Compléter le cadre juridique en matière de prévention et de répression du terrorisme

Depuis la censure par le Conseil constitutionnel du délit de recel d'apologie du terrorisme en 2020, l'arsenal juridique français ne permet plus de poursuivre une personne qui détiendrait de documents ou images apologétiques.

La création d'une infraction permettant de sanctionner des individus détenant de tels contenus pourrait être envisagée dès lors que deux conditions cumulatives sont réunies : un critère de gravité associé à un élément intentionnel.

Afin de tenir compte d'une exigence constitutionnelle, cette infraction ne sanctionnerait pas la détention de contenus apologétiques de manière générale, mais uniquement la détention des contenus les plus graves, exhibant des crimes terroristes.

Par ailleurs, la création d'une **interdiction de paraître en cas d'événements exposés à des actes de terrorisme** permettrait de contourner l'impossibilité actuelle de prononcer une interdiction de paraître à l'encontre d'individus ayant déjà été placés sous MICAS pendant 12 mois.

d. Renforcer l'arsenal juridique en matière de lutte contre la criminalité organisée

L'élargissement, au moins à titre expérimental, de la technique de l'algorithme à la finalité 6 (prévention de la criminalité et de la délinquance organisées) serait de nature à faciliter l'accès des services dans ce domaine. *****.

e. Faciliter la lutte contre la fraude fiscale

L'intégration des délits de fraudes fiscales prévus aux articles 1741 à 1744 du Code général des impôts, aux incriminations pénales énumérées aux articles 706-73 et 706-73-1 du Code de procédure pénale permettrait au renseignement douanier et plus particulièrement à la nouvelle unité de renseignement fiscal de solliciter, au titre de la finalité 6 (prévention de la criminalité et de la délinquance organisées) de l'article 811-3 du CSI, des techniques de renseignement au profit de leurs enquêtes.

Par ailleurs, un élargissement du mécanisme légal de « renseignarisation » des informations judiciaires à la matière fiscale, en particulier celles collectées dans le cadre des enquêtes menées par le PNF, serait de nature à améliorer l'efficacité de l'action de l'État dans la lutte contre la grande fraude fiscale.

f. Se prémunir des ingérences étrangères

Dans le contexte de tentatives croissantes d'ingérences étrangères sur le territoire national, certaines puissances recherchent la collaboration d'agents publics dont l'expertise technique ou le savoir-faire opérationnel présente un intérêt stratégique.

Alors que la dernière loi de programmation militaire a instauré un régime de contrôle des départs à l'étranger de militaires, une réflexion pourrait être engagée sur la pertinence - ou non - d'étendre ce régime aux agents civils de l'État et de ses établissements publics qui exercent des fonctions d'une sensibilité particulière ou disposent de compétences spécialisées.

À des fins de prévention des ingérences étrangères, il pourrait également être pertinent de permettre la communication d'éléments issus de procédures judiciaires aux services de renseignement, à l'instar de ce qui a été prévu dans le cadre de la prévention du terrorisme.

g. Veiller au respect de la déontologie des agents des services de renseignement

Au vu de certaines pratiques de nature à compromettre le secret de la défense nationale, une obligation de déclaration pourrait être imposée aux agents actifs et retraités d'un service de renseignement désirant publier un ouvrage sur leurs activités professionnelles.

C. PENSER NOTRE AUTONOMIE STRATÉGIQUE À L'ÉCHELLE EUROPÉENNE

L'idée d'autonomie stratégique européenne s'est imposée comme un des thèmes majeurs du débat politique et sécuritaire depuis une décennie. Elle renvoie à la capacité des Européens à agir par eux-mêmes, à défendre leurs intérêts, à protéger leurs citoyens et à anticiper les menaces sans dépendre intégralement de puissances extérieures. Longtemps cantonnée aux domaines militaires ou industriels, cette autonomie doit aujourd'hui s'étendre résolument au champ du renseignement, qui en constitue à la fois le socle et la condition d'efficacité.

1. Un constat : des coopérations européennes à géométrie et à intérêt variables

Il n'existe pas d'Europe du renseignement au sens d'une politique publique portée par l'Union européenne, l'article 4.2 du Traité de l'Union européenne disposant que « *la sécurité nationale reste de la seule responsabilité de chaque État membre* ». **Le renseignement demeure sans ambiguïté une compétence souveraine des États membres.**

On dénombre toutefois de multiples instances et modalités de coopération entre les services de renseignement à l'échelle européenne, qui sont à géométrie variable selon les thématiques traitées et les zones géographiques couvertes. Dans tous les cas de figure, la coopération intervient dans le cadre des législations nationales et dans le plus grand respect de la protection des données sensibles.

a. Un cadre de coopération multilatérale global qui reste limité

i. Au sein de l'Union européenne

Le cadre de coopération établi au sein des institutions européennes est celui de la SIAC (*Single Intelligence Analysis Capacity*), cette capacité intégrée d'analyse du renseignement de l'Union européenne. Il ne s'agit pas d'un service ou d'une agence autonome, mais bien d'un cadre de coopération qui réunit deux entités existantes :

– **Une composante civile :** *****. *L'IntCen*, qui réunit essentiellement d'experts nationaux détachés issus des services des États membres, ***** afin d'en faire la synthèse et de la diffuser aux autorités compétentes, au premier chef le Service européen d'action extérieure (SEAE). *****.

– **Une composante militaire** : la direction du renseignement de l'État-major de l'UE (EUMS INT).

Ensemble, ces deux composantes produisent des analyses stratégiques destinées aux institutions de l'Union européenne. La SIAC ne collecte pas de renseignement propre : il exploite les informations transmises volontairement par

les services des États membres, ainsi que des sources ouvertes et diverses informations institutionnelles.

Le renseignement français est un contributeur majeur de l'*IntCen*, à qui sont transmises sur initiative ou sur demande des notes de renseignement relatives aux thématiques traitées par les services français.

Le renseignement fusionné que produit la SIAC n'apportant pas toujours une forte valeur ajoutée pour les services français, ceux-ci, en lien avec la CNRLT, ont à cœur d'en **renforcer le positionnement et la pertinence,** en s'attachant à la qualité de ses contributions en renseignement, en y augmentant leur présence et en diversifiant leurs interactions avec celui-ci.

Le renforcement de la prise en compte du renseignement par L'UE implique en effet une montée en puissance de la SIAC ; **c'est l'objectif fixé par les chefs d'État et de gouvernement dans la boussole stratégique de 2022**. Ce document cadre de la stratégie internationale européenne a en effet consacré la SIAC comme point d'entrée unique du renseignement stratégique au sein des institutions européennes et demande ainsi son renforcement.

La communauté du renseignement est en revanche très hostile à une immixtion de la Commission européenne dans le champ du renseignement, compétence exclusive des États membres. Or il semble qu'au vu de l'évolution du contexte géopolitique, la Commission semble vouloir se doter de nouvelles compétences, notamment celle de disposer d'analyses des risques et des menaces, dont l'objectif plus ou moins affiché serait à terme de disposer d'une capacité propre et autonome de production de renseignement. Or les services de renseignement considèrent particulièrement préjudiciable que la Commission européenne veuille ainsi orienter de façon directe l'activité des services de renseignement nationaux. Dans ce contexte, **les autorités françaises ont transmis un *non-paper* sur le renseignement à destination des décideurs européens**. Ce document insiste sur la préservation du rôle de la SIAC dans le dispositif de renseignement européen.

Par ailleurs, ***** créé à l'initiative de la France en 2019, permettent de rapprocher les communautés européennes du renseignement et de renforcer la culture stratégique européenne.

ii. Au sein de l'OTAN

À l'OTAN, les interactions avec les services de renseignement s'effectuent dans le cadre du Comité de renseignement civil de l'OTAN (CIC, *Civilian Intelligence Committee*). La DGSI, conjointement avec la DGSE, représente la France dans cette instance. Ce Comité est un espace de travail au sein duquel les services civils alliés produisent des synthèses destinées à la prise de décision collective, essentiellement au niveau du Conseil de l'Atlantique Nord.

Ce comité est subordonné au principal organe de décision politique de l'OTAN : le Conseil de l'Atlantique Nord. Le Conseil, présidé par le Secrétaire général de l'OTAN, peut se réunir au niveau des représentants permanents (ambassadeurs), au niveau des ministres de la Défense et des Affaires étrangères, et au niveau des chefs d'États et de gouvernement (en format « Sommet », tous les deux ans).

Force est de constater que **la prédominance otanienne dans le paysage du renseignement multilatéral sur le continent européen constitue un frein à une forme d'intégration européenne en matière de renseignement**.

b. Des coopérations thématiques plus ciblées et plus opérationnelles

Eu égard aux spécificités propres au champ du renseignement, la dynamique de coopération ne concerne pas uniformément les services des 27 États membres. Le degré de partage des informations dépend en premier lieu de la thématique traitée et repose avant tout sur la confiance, le niveau de sécurité, de capacités opérationnelles et techniques ainsi que la convergence des cibles prioritaires.

Aucun service ne partage de renseignement avec un partenaire s'il estime que ce dernier n'a pas besoin de ce renseignement et/ou que les failles de sécurité de ce service sont susceptibles de porter atteinte à la source de ce renseignement. Les contacts et les échanges entre services européens sont suffisamment denses pour que chacun connaisse les centres d'intérêt respectifs des autres services.

*****.

Dans le domaine du renseignement militaire, les échanges se font dans la grande majorité des cas à l'échelon bilatéral. Cependant, des coalitions *ad hoc* se mettent en place dans le cadre de la guerre en Ukraine : elles permettent à certains services européens détenant une compétence précise de mettre en commun leur capacité sur un sujet spécifique et, ainsi, de rationaliser l'effort de manière constructive. Bien que balbutiantes, **ces coalitions offrent de premiers résultats probants,** qui invitent à développer davantage ce format d'échanges. Sur le plan de l'influence, elles permettent à la France d'asseoir son rôle de nation-cadre.

Grâce à leurs coopérations, les partenaires européens opèrent un suivi sur l'ensemble du globe. Sans détenir le niveau d'expertise des services de renseignement américains, les coopérations européennes permettent ainsi de partager, confronter et compléter les analyses des services français sur de nombreuses thématiques. Dans le champ du renseignement militaire, le développement des relations partenariales permet, depuis plusieurs années, de renforcer le maillage de la DRM à travers le déploiement de capteurs temporaires et permanents sur le territoire national de plusieurs pays européens, plus particulièrement sur le flanc Est. Ces campagnes de recueil accroissent considérablement les compétences et capacités d'anticipation de la DRM.

S’agissant du renseignement douanier, la DNRED dispose de deux canaux d’échange privilégiés qui sont la **Convention dite Naples 2 et Europol**. Nul partage dans ces enceintes de renseignement classifié issu notamment de la mise en œuvre de techniques de renseignement, mais davantage une coopération avec les services de douane, gendarmerie ou police d’autres pays européens. S’agissant du renseignement au sens strict du terme, la DNRED peut échanger *via* les services partenaires de la communauté française du renseignement ou *via* le réseau d’attachés douaniers en poste dans les États membres.

En matière de sanctions, de trafics de biens culturels ou d’espèces protégées, la DNRED coopère de façon fluide et quotidienne avec ses partenaires européens. S’agissant de la lutte contre le trafic de stupéfiants, **la réforme de l’Union douanière qui implique la création d’une autorité douanière européenne s’avère déterminante**, tant l’action des Européens doit être concertée et fondée sur les mêmes standards.

Dans le champ de compétences de Tracfin, la création de **l’Autorité européenne de lutte contre le blanchiment des capitaux** (AMLA), opérationnelle depuis le 1er juillet 2025, ouvre de nouvelles perspectives. Tracfin entretient depuis longtemps des relations denses avec ses homologues européens. En 2024, les échanges de Tracfin avec les services partenaires européens ont ainsi représenté 67 % de ses échanges internationaux. Le rôle la nouvelle agence européenne, dont le siège est à Francfort, vise à garantir une application cohérente et uniforme des règles anti-blanchiment dans tous les États membres, là où auparavant chaque pays avait son propre dispositif.

La création de l’AMLA ne remplace pas les structures nationales comme Tracfin mais les complète en jouant un rôle de superviseur européen, en facilitant la coopération internationale et l’harmonisation des pratiques. En cas de détection d’activités suspectes, Tracfin conserve son rôle d’« intelligence financière nationale », mais pourra désormais s’appuyer sur l’AMLA pour des cas transnationaux ou des entités diffuses (cryptoactifs, prestataires de services à distance, etc.).

2. Une ambition : atteindre une autonomie stratégique européenne dans le respect des souverainetés nationales

Le **rapport Niinistö**, intitulé *Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness*, a été remis le 30 octobre 2024 à la Commission européenne. Il vise à évaluer les défis complexes que l’Union européenne et ses États membres affrontent dans un monde marqué par des crises variées : guerre, cyberattaques, menaces hybrides, pandémies, crises énergétiques, instabilités géopolitiques, etc. Son ambition est d’instaurer une « préparation globale » (civile et militaire) au niveau européen, c’est-à-dire la capacité de l’Union à anticiper, prévenir, résister et répondre à tout type de crise ou menace.

Le rapport souligne que les **divergences existantes entre États membres –** en matière de pratiques de contre-espionnage, de législation, de partage d'information transfrontalier – constituent aujourd'hui une vulnérabilité dès lors que des acteurs malveillants peuvent en profiter. Pour y remédier, **l'idée d'une agence de renseignement européenne est évoquée,** plus précisément, une structure de coopération du renseignement au niveau de l'Union, destinée à répondre à des besoins stratégiques et opérationnels. **Cependant, le rapport souligne les obstacles forts :** de nombreux États membres considèrent le renseignement comme un domaine de souveraineté nationale. Même si la création d'une telle agence supranationale est jugée peu probable à court terme, **le rapport insiste pour développer un cadre européen d'échange d'information sensible, de contre-espionnage partagé, d'analyse commune et de solidarité en matière de sécurité.**

Ce rapport met ainsi en avant la nécessité **d'une coopération renforcée entre les institutions civiles et militaires**, ainsi qu'une planification conjointe entre États membres pour faire face aux menaces transversales. **Le rapport considère la préparation comme un « bien public »**, ce qui implique non seulement des États, mais aussi des institutions européennes, des acteurs privés (entreprises, infrastructures critiques) et la société civile. Il plaide pour des mécanismes institutionnels pérennes : exercices réguliers transnationaux, coordination civile-militaire, plans d'urgence coordonnés, surveillance (espionnage d'État, observation satellitaire, renseignement géospatial, etc.), ainsi qu'un financement durable afin de garantir la résilience même dans des crises majeures.

Les conclusions de ce rapport sont loin de faire l'unanimité au sein des États membres et les services de renseignement qui craignent une mainmise de l'Union européenne sur une compétence qui doit rester exclusivement nationale. **Les préconisations du rapport Niinistö se heurtent à plusieurs obstacles :** la diversité des traditions nationales en matière de renseignement, la réticence de certains États à céder des prérogatives souveraines, le manque de confiance mutuelle, et la complexité structurelle d'instituer une coopération européenne approfondie dans des domaines sensibles.

Pour autant, la quête d'une autonomie stratégique européenne ne peut se résoudre au *statu quo*. Elle suppose de toujours mieux partager ce qui peut l'être, de manière sécurisée et en respectant les sensibilités nationales. **Il ne doit nullement s'agir de créer une « CIA européenne », perspective irréaliste et politiquement inacceptable pour la plupart des États**, mais bel et bien de parachever une architecture d'analyse commune, fondée sur la mutualisation de données, la standardisation des formats de renseignement, la montée en puissance d'outils communs (satellitaires, cyber, intelligence économique) et *****.

Cette coopération doit permettre aux dirigeants européens d'accéder à des évaluations convergentes, produites par un dispositif robuste, crédible, capable d'alerter rapidement sur des signaux faibles, de détecter les opérations hostiles et de proposer des réponses coordonnées. Dans un espace politique souvent marqué par

des perceptions divergentes des menaces – Russie, Chine, terrorisme, instabilités régionales – une telle convergence renforcerait la cohérence stratégique et la solidarité entre États membres.

*****. Les capacités d'analyse des données massives, de cryptographie, de renseignement spatial ou de contre-ingérence nécessitent des technologies maîtrisées, souveraines, et un écosystème industriel capable d'innover rapidement. Sans cela, l'Europe reste tributaire d'outils étrangers pour produire ou sécuriser ses propres informations sensibles, ce qui fragilise sa capacité de décision autonome.

Il s'agit aussi **d'inscrire le renseignement dans une logique de résilience stratégique :** protéger les infrastructures critiques, surveiller les chaînes d'approvisionnement, anticiper les ruptures, détecter les menaces hybrides avant qu'elles n'atteignent un seuil de crise. L'autonomie stratégique commence en réalité en amont, dans la capacité à prévoir plutôt qu'à réagir.

Enfin, penser l'autonomie stratégique européenne dans le champ du renseignement exige **un effort de culture commune**. Cela passe par la formation, les échanges de personnels, les exercices conjoints, une meilleure compréhension mutuelle entre services et une volonté politique de dépasser les réticences historiques. Le renseignement, souvent perçu comme un domaine opaque et strictement national, doit devenir un instrument de confiance partagée au sein d'une Europe qui cherche à se protéger collectivement.

En définitive, **la construction d'une autonomie stratégique européenne repose moins sur des structures spectaculaires que sur une écologie du renseignement :** ***** partage maîtrisé, analyse collective, technologies souveraines et culture de coopération. À cet égard, **un premier investissement européen mutualisé pourrait être envisagé pour la création d'un système d'information visant à échanger des données classifiées de niveau « Secret UE »** à l'image de ce que propose le système d'information américain *****. La mise en place d'un tel système d'information, indépendant des systèmes américains, serait un prérequis à toute avancée concrète en termes de partage multilatéral de renseignement au niveau strictement européen.

RECOMMANDATIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT AU TITRE DE SON RAPPORT ANNUEL 2025

Recommandation n° 1 : Dans le contexte budgétaire actuel, sans préjuger des efforts de gestion et de rationalisation demandés à toute administration publique, préserver les crédits alloués à la communauté du renseignement qui, au vu leurs montants, ne doivent pas servir de variable d'ajustement aux arbitrages politiques liés à l'objectif de réduction des déficits publics. L'actualisation de la loi de programmation militaire prévue en 2026 doit confirmer la priorité budgétaire donnée à la politique publique du renseignement.

Recommandation n° 2 : Engager les adaptations juridiques nécessaires pour faire face à l'élévation du niveau de haute intensité des menaces et de leurs évolutions technologiques (messageries cryptées, algorithmes, ***** etc.).

Recommandation n° 3 : Garantir le socle de notre autonomie stratégique autour de programme capacitaires souverains et d'alliances et partenariats diversifiés.

Recommandation n° 4 : Alors que la technologie occupe une place croissante dans les métiers du renseignement, il est essentiel de ne pas sous-estimer la valeur irremplaçable de la dimension humaine. Cela rend nécessaire d'œuvrer à l'attractivité et la fidélisation des talents au sein de la communauté du renseignement, en particulier par la mise en place d'un régime indemnitaire adapté, équitable et compétitif, tenant compte des contraintes inhérentes aux métiers du renseignement et de la rareté de certains profils essentiels pour la communauté du renseignement.

Recommandation n° 5 : *****.

Recommandation n° 6 : Définir le cadre stratégique d'une coopération structurée en matière de sécurité entre l'Union européenne et le Royaume-Uni.

Recommandation n° 7 : Doter l'Union européenne d'un système d'information sécurisé visant à échanger des données classifiées de niveau « Secret UE » à l'image du système d'information américain *BICES*.

Recommandation n° 8 : Au regard des défis majeurs posés par les nouvelles formes de menaces, il est indispensable de promouvoir un véritable débat démocratique autour des enjeux actuels et futurs en créant les conditions d'un débat national plus large, associant représentants élus, experts, acteurs institutionnels et société civile. Une telle démarche favoriserait la transparence, l'adhésion citoyenne et la légitimité démocratique des actions menées, tout en contribuant à la diffusion d'une véritable culture de défense et de sécurité nationale.

Recommandation n° 9 : Mettre en œuvre la disposition de la loi du 25 juillet 2024 visant à prévenir les ingérences étrangères en France, qui prévoit la remise par le Gouvernement au Parlement d'un rapport sur l'état des menaces pesant sur la sécurité nationale, pouvant donner lieu à un débat parlementaire en séance publique.

Recommandation n° 10 : Associer la délégation parlementaire au renseignement, le plus en amont possible, à la réflexion qu'entend engager le ministère de l'intérieur sur la lutte contre l'entrisme, au vu de la dimension politique, juridique et technique du sujet.

CHAPITRE IV :
RAPPORT GÉNÉRAL DE LA CVFS SUR LES CONDITIONS D'EMPLOI DES FONDS SPÉCIAUX AU COURS DE L'EXERCICE 2024

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 ».

La Commission a procédé, au cours de l'année 2025, au contrôle des comptes de l'exercice budgétaire 2024. Elle est composée comme suit :

– M. Aurélien Rousseau, député (App. SOC) des Yvelines, Président.

– Mme Catherine Di Folco, sénateur (LR) du Rhône (jusqu'en mars 2025) puis Mme Agnès Canayer, sénateur (LR) de la Seine-Maritime depuis mars 2025.

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

– Mme Gisèle Jourda, sénatrice (SER) de l'Aude.

Pour mener sa mission et élaborer son rapport annuel, 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. De mai à décembre 2025, elle s'est ainsi rendue :

– au groupement interministériel de contrôle (GIC) le 20 mai 2025 ;

– à la direction générale de la sécurité intérieure (DGSI) le 21 mai 2025 ;

– à la direction nationale du renseignement et des enquêtes douanières (DNRED) le 27 mai 2025 ;

– à la direction du renseignement et de la sécurité de la défense (DRSD) le 28 mai 2025 ;

– à la direction générale de la sécurité extérieure (DGSE) les 4 juin et 2 octobre 2025 ;

– à la direction du renseignement militaire (DRM) et au Commandement des opérations spéciales (COS) le 11 juin 2025 ;

– au service national du renseignement pénitentiaire (SNRP) le 12 juin 2025 ;

– à Tracfin le 12 juin 2025 ;

– à la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) le 17 décembre 2025.

La CVFS a également effectué deux déplacements hors siège :

– l'un à l'étranger, du 25 au 28 mars 2025

– l'autre à Marseille, les 21 et 22 octobre 2025 auprès des directions zonales de la DGSI, de la DNRED, et à la CIRP du SNRP.

———

La Commission de vérification des fonds spéciaux a connu une activité soutenue au cours de l'année 2025. Elle s'est rendue dans chacun des services de renseignement et structures bénéficiaires de fonds spéciaux pour effectuer ses contrôles sur place et sur pièces. Elle a aussi souhaité, au-delà des échelons centraux, se déplacer dans des directions zonales à Marseille auprès de la DGSI, de la DNRED et du SNRP et a visité plusieurs postes *****. Ces temps d'échange avec les praticiens des fonds spéciaux se sont révélés particulièrement utiles pour évaluer la valeur ajoutée opérationnelle de ces fonds dans le travail quotidien des agents des services de renseignement.

L'examen des comptes de l'exercice budgétaire 2024, objet de ce rapport, confirme la phase de maturité qui caractérise désormais la gestion des fonds spéciaux, laquelle obéit à une doctrine bien établie et à un cadre de gestion rigoureux dans chacune des structures concernées. De ce fait, et même si quelques anomalies de gestion subsistent, notamment en matière d'anonymisation, l'intérêt du contrôle effectué par la CVFS concerne moins l'analyse des pièces comptables que des problématiques transversales et souvent communes à l'ensemble des services.

Parce ce que les élus qui la composent sont aussi membres de la Délégation parlementaire au renseignement, la CVFS prend ainsi toute sa part à un contrôle effectif de la politique publique du renseignement et apporte un éclairage fort utile aux travaux de la DPR.

La CVFS souhaite cette année attirer l'attention sur les sujets suivants :

– **L'insincérité manifeste du montant des fonds spéciaux inscrits en loi de finances initiale**, au programme budgétaire 129. Elle se confirme et s'amplifie au fil du temps. ***** La Commission réitère l'exigence de réserver les DDAI à des besoins réellement imprévisibles. Pour sortir de l'insincérité budgétaire, la CVFS appelle à un resoclage autour de 100 millions d'euros du montant des fonds inscrits en loi de finances initiale.

– **Le niveau de trésorerie disponible** de plusieurs services, *****, se situe fin 2024 à un niveau plancher préoccupant. Si la résorption des reliquats de trésorerie a été pendant plusieurs années la variable d'ajustement légitime

du montant des dotations allouées aux services, force est de constater que le seuil d'alerte a été atteint, pouvant potentiellement compromettre la continuité de l'activité opérationnelle des services. À cet égard, le « coup de rabot » opéré sur les dotations 2024 au titre de la contribution du renseignement à la résorption des déficits publics interroge. Au regard des montants en jeu, il eut été plus pertinent de faire porter cet effort exclusivement sur les fonds normaux.

– **La perspective à la baisse des besoins en fonds spéciaux interroge**, au vu du contexte international et des implications liées à la mise en œuvre de la nouvelle *Revue nationale stratégique* adoptée à l'été 2025. Alors que les dépenses en fonds spéciaux sont en hausse continue et significative depuis la fin du Covid, les expressions de besoins de fonds spéciaux jusqu'en 2028 sont contradictoires avec l'ambition assignée à la communauté du renseignement, qui plus est dans un contexte où les reliquats de trésorerie disponible des services sont désormais apurés.

– Les services, avec l'appui indispensable de la CNRLT, doivent travailler à la modalisation dans la durée de leurs besoins en fonds spéciaux liés au **maintien en conditions opérationnelles (MCO)** des matériels ou dispositifs techniques acquis en fonds spéciaux. L'anonymisation doit en effet se concevoir sur tout le cycle de vie des matériels acquis en fonds spéciaux. Cette charge financière rigidifie la consommation des fonds spéciaux et doit faire l'objet d'un traitement comptable spécifique.

– **Une forme de non-recours aux fonds spéciaux** a été constatée par la commission. Alors que processus de « fond-normalisation » semble arriver à son terme, la CVFS observe *a contrario* que, faute de culture suffisante des fonds spéciaux au niveau des échelons territoriaux, *****. La connaissance de la doctrine d'emploi des fonds spéciaux mériterait d'être davantage partagée, dans l'intérêt des services et pour sécuriser leurs opérations *****.

– **L'accélération du phénomène de dématérialisation des paiements** rend de plus en plus complexe le recours aux fonds spéciaux, en particulier dans certains pays ***** où les transactions en espèces attirent l'attention au lieu de garantir la discrétion. Il serait utile de définir un cadre commun de développement des instruments de paiement démarqués afin d'éviter des pratiques trop hétérogènes d'un service à l'autre.

– La dématérialisation de pièces comptables liées à l'utilisation des fonds spéciaux, dans le cadre du déploiement de nouveaux logiciels de gestion, appelle à **définir une doctrine liée aux règles de conservation des pièces comptables**. La CNRLT pourrait utilement réaliser un audit des pratiques actuelles en vue d'une harmonisation des règles d'archivage.

– *****.

– Au vu des problématiques transversales et communes à de nombreux services, la CVFS appelle la CNRLT à prendre la mesure de l'attente des services et de la nécessaire permanence du **groupe de travail sur les fonds spéciaux** pour avancer des solutions opérationnelles, au-delà d'un lieu d'échanges informels.

Tels sont les principaux enseignements issus des contrôles sur place et sur pièces effectués par la CVFS sur les conditions d'emploi des fonds spéciaux. Treize nouvelles recommandations sont formulées au titre de l'exercice 2024.

Aurélien ROUSSEAU
Député des Yvelines,
Président de la Commission de vérification des fonds spéciaux

NOUVELLE RECOMMANDATION GÉNÉRALE ÉMISE PAR LA CVFS

Recommandation générale n° 2024-01 : Évaluer les besoins en fonds spéciaux nécessaires à la mise en œuvre des attendus de la *Revue nationale stratégique*.

EXAMEN PAR LA DÉLÉGATION

Réunie le mardi 16 décembre 2025 sous la présidence de M. Jean-Michel Jacques, la Délégation a procédé à l'examen de son rapport annuel.

Après un exposé de son président, la Délégation a adopté son rapport d'activité au titre de l'année 2025 (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 a entendu le 15 janvier 2026 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

Les bouleversements géopolitiques et la vitesse de transformation du monde confèrent au renseignement un rôle majeur pour garantir notre autonomie décisionnelle et l'exercice effectif de la souveraineté nationale.

Le retour à un monde de confrontations est marqué par l'addition des menaces, leur renforcement et leur imbrication mutuelle. Le contexte international n'est pas sans influence sur la permanence d'une menace terroriste à un haut niveau d'intensité. La criminalité organisée fait appel à des moyens de plus en plus sophistiqués qui font des narcotrafiquants de véritables compétiteurs pour les États. Les atteintes à la sécurité économique sont elles aussi de plus en plus nombreuses et ciblent en particulier notre base industrielle et technologique de défense, engagée dans le soutien militaire à l'Ukraine.

À ces menaces « classiques » viennent s'en ajouter de nouvelles, souvent qualifiées d'hybrides en raison de modes opératoires protéiformes utilisés à des fins de déstabilisation. Les ingérences étrangères sont le fait de puissances hostiles qui investissent notamment l'espace numérique pour en faire le champ de bataille de la guerre informationnelle.

L'état de la menace, conjuguée à l'instabilité internationale, n'est pas sans conséquences sur la communauté du renseignement. La situation sécuritaire au Sahel a rebattu les cartes de l'implantation de nos services dans cette partie de l'Afrique. La guerre en Ukraine a pour sa part conduit à un redéploiement d'une partie de nos moyens sur le flanc Est de l'Europe. L'activité quotidienne des services de renseignement est directement impactée par les conflits en cours, par exemple dans la mise en œuvre des sanctions infligées à la Russie.

Cette nouvelle donne géopolitique a conduit à la mise à jour de notre doctrine stratégique avec la publication à l'été 2025 d'une nouvelle revue stratégique nationale (RNS) qui confère au renseignement un rôle central face à la dangerosité du monde. La RNS fait écho à la stratégie nationale du renseignement adoptée en janvier 2025, feuille de route de la communauté française du renseignement, sous la responsabilité du coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT).

Cette doctrine constitue le cadre stratégique d'un nouveau cycle du renseignement français. Celui-ci est marqué par de nouvelles méthodes de travail, adossées à de profondes réorganisations internes, fondées sur le décloisonnement et la transversalité. Le temps de la guerre des services est clairement révolu, laissant place à des coopérations interservices et des mutualisations opérationnelles toujours plus nombreuses, tant sur le plan technique qu'en matière de ressources humaines. La priorité donnée au renseignement se traduit par des moyens budgétaires accrus, à contre-courant des efforts demandés au pays pour réduire les déficits publics.

Pour développer et renforcer une capacité autonome de renseignement, il s'agit de limiter nos dépendances sans pour autant renoncer aux alliances, car dans le monde du renseignement, l'autarcie n'est ni souhaitable, ni réaliste. Les échanges partenariaux sont toujours réalisés dans une logique de troc, selon une démarche de confiance et de réciprocité. Les changements géopolitiques ont progressivement redessiné la cartographie des alliances et des partenariats. Alors que les États-Unis viennent de publier leur nouvelle stratégie de sécurité nationale, qui réévalue leur relation avec l'Europe, il y a urgence à limiter notre dépendance à l'Amérique et à réduire autant que possible le recours à des solutions techniques étrangères.

Doter le renseignement français de nouvelles capacités autonomes ne peut s'envisager que dans le strict respect des exigences de l'État de droit. C'est la force d'une démocratie, même si cela crée, il est vrai, une asymétrie juridique avec les services de renseignement qui opèrent dans des régimes autoritaires. Dix ans après l'entrée en vigueur du cadre légal défini par la loi renseignement de 2015, le bilan tiré par les services de renseignement et leurs autorités de contrôle est largement positif. L'exigence démocratique repose sur un juste équilibre entre efficacité opérationnelle et respect des libertés fondamentales. L'intensité de la menace, associée aux évolutions technologiques, conduit toutefois à envisager des évolutions à apporter au régime juridique de la collecte du renseignement, en particulier pour l'accès aux communications chiffrées.

Diverses mesures de modernisation ou d'ajustement, relatives au cadre d'emploi des techniques de renseignement et aux modalités d'exploitation et de conservation des données qui en sont issues, semblent également nécessaires. Quant à la jurisprudence européenne de la cour de justice de Luxembourg et de la Cour européenne des droits de l'Homme de Strasbourg, elle est un motif de préoccupation des services de renseignement au vu des limites posées à la conduite de leurs investigations.

Face à la vitesse des évolutions technologiques, la communauté du renseignement doit se mettre en ordre de marche pour éviter le décrochage. Cela concerne principalement les domaines tels que l'intelligence artificielle, le quantique mais aussi du secteur spatial, de plus en plus stratégique. La France doit investir dans des capacités souveraines qu'il s'agisse des systèmes de sécurité et d'information, de programmes capacitaires, de renseignement en sources ouvertes (OSINT). Mais la technologie n'est pas tout ; la communauté du renseignement repose des femmes et des hommes, ce qui rend nécessaire de renforcer l'attractivité des métiers du renseignement, dans un contexte de forte concurrence avec le secteur privé.

Enfin, l'autonomie stratégique dépasse le périmètre des frontières nationales et doit se penser l'échelle européenne, dans le respect des souverainetés nationales, le traité de l'Union européenne disposant que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cela n'interdit pas des coopérations européennes qui sont à géométrie et à intérêt variables. Des coopérations thématiques et opérationnelles existent depuis longtemps et fonctionnent bien, en particulier dans les domaines de l'antiterrorisme, du renseignement douanier et de la lutte contre le blanchiment. Il s'agit à présent de franchir une nouvelle étape alors que la proposition de la Commission européenne de se doter l'Union européenne de sa propre unité de renseignement est rejetée de toutes parts.

Au terme de son rapport, la Délégation parlementaire au renseignement formule dix recommandations visant à conforter la place du renseignement au service de notre autonomie stratégique et de l'exercice effectif de la souveraineté nationale.