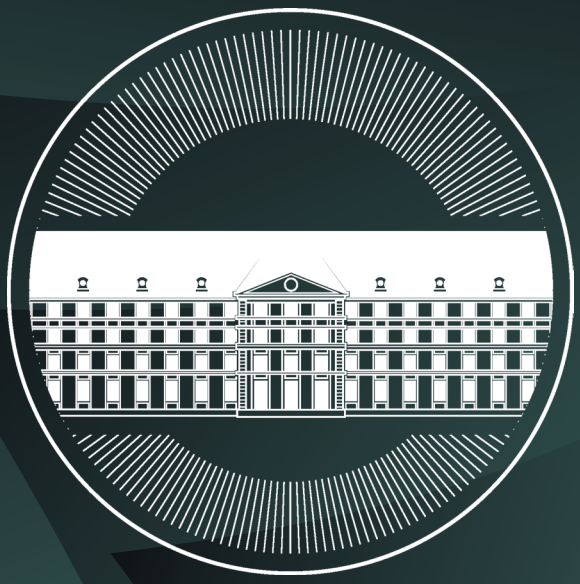
PREMIER
MINISTRE

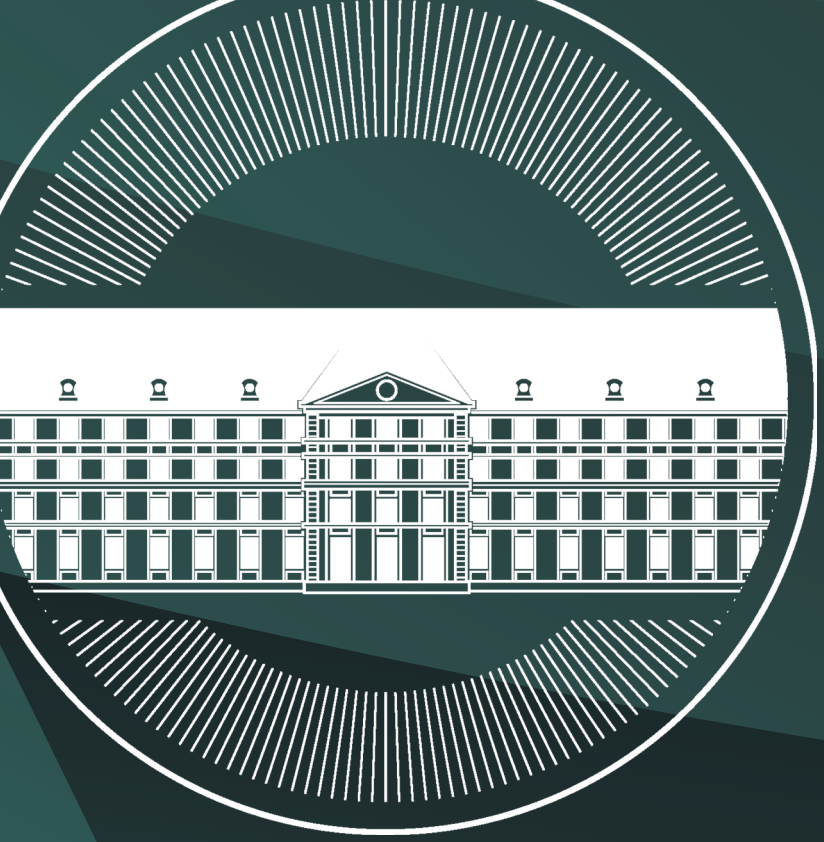
Liberté
Égalité
Fraternité



RAPPORT D'ACTIVITÉ

2025

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE
ET DE LA SÉCURITÉ NATIONALE



Secrétariat général de la défense
et de la sécurité nationale

Édité par le Secrétariat général de la défense et de la sécurité nationale (SGDSN)

Directeur de la publication :
Nicolas Roche

Coordination :
Gwénaël Jézéquel

Conception et réalisation :
Louise Laurent

Coordination éditoriale :
Justine Boquet

Crédits photo :

SOMMAIRE

5
ÉDITO

7
ORGANIGRAMME

8
ÉLÉMENTS
DE CHRONOLOGIE 2025

10
ACTUALISATION DE LA REVUE
NATIONALE STRATÉGIQUE

15
FAIRE FACE
À DES MENACES NOUVELLES

23
CONSOLIDER LA POSITION
INTERMINISTÉRIELLE

33
RENFORCER LE NIVEAU
DE PRÉPARATION

39
PARTICIPER À LA CONTINUITÉ
DE L'ÉTAT

45
DÉVELOPPER DE NOUVELLES
CAPACITÉS

53
PRENDRE EN COMPTE UN
ENVIRONNEMENT EN MOUVEMENT

57
ACCOMPAGNER LA RÉFLEXION
DES AUTORITÉS

63
SOUTENIR L'ACTIVITÉ

4

ÉDITO

Nicolas ROCHE

Secrétaire général de la défense
et de la sécurité nationale

Du point de vue du SGDSN, l'année 2025 aura été indéniablement marquée par un intense travail interministériel de révision stratégique.

Le cœur de cet effort aura été l'actualisation de la Revue nationale stratégique, commandée par le Président de la République à l'occasion de ses vœux aux armées. Sans qu'aucun des travaux et missions habituels n'aient été interrompus, cette révision aura constitué un axe d'effort particulièrement important tout au long du premier semestre. Elle aura permis d'éprouver une nouvelle méthode, à la fois rapide, collaborative, approfondie et opérationnelle rompant avec les longs travaux antérieurs de livre blanc avec des réflexions plus courtes mais impliquant peu d'acteurs.

De fait, l'ensemble des ministères auront été impliqués dans un travail qui vise à tirer les conséquences des désordres mondiaux affectant l'ensemble des domaines de la vie de la Nation. Au-delà des services de l'État, les groupes de réflexion et divers experts auront été auditionnés et nos voisins britanniques et allemands auront été sollicités avant la finalisation des travaux. A l'issue d'une première phase qui aura permis d'aboutir à une version préliminaire, les associations d'élus et les commissions en charge de la défense à l'Assemblée nationale et au Sénat ont été saisies en vue de recueillir leurs propositions d'amendement. Les modifications qu'elles ont souhaité voir figurer dans la stratégie nationale ont été intégrées au document final. Cette démarche inédite aura permis de constater que, au-delà de divergences politiques connues, la démarche de rénovation stratégique et les conclusions proposées par le groupe de travail interministériel animé par le SGDSN faisaient l'objet d'un très large consensus. ▸▸▸

ÉDITO

Nicolas ROCHE

Secrétaire général de la défense
et de la sécurité nationale

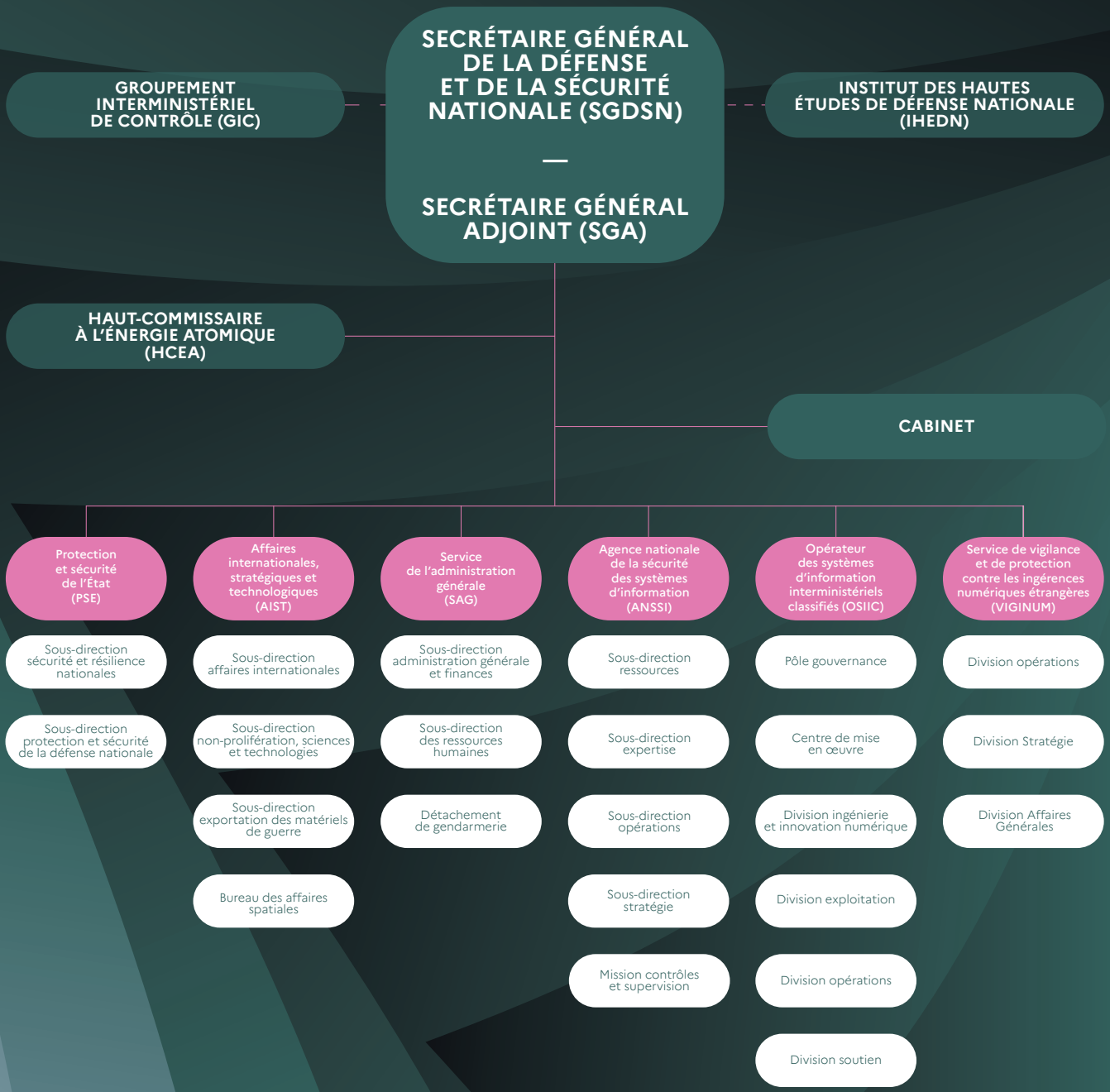
La stratégie finalisée, approuvée par le Président de la République et le Premier ministre, a été publiée le 14 juillet et, à travers les onze objectifs qu'elle fixe, guide depuis lors notre action. Ce travail a été très largement complété par la publication d'un nombre important de documents officiels, majoritairement en 2025 mais aussi durant le premier trimestre de l'année 2026. Ainsi, la stratégie nationale de résilience qui datait de 2022 a été actualisée pour tenir compte des inflexions nouvelles portées par la Revue stratégique. Une stratégie nationale spatiale pour la période 2025-2040 a été publiée au mois de novembre. La stratégie nationale de cybersécurité, datant de 2018, a aussi été actualisée et une nouvelle version est parue au mois de janvier. Le mois suivant est parue la première stratégie nationale de lutte contre les manipulations de l'information 2026-2030. Toujours en février 2026 a été dévoilée la première feuille de route de l'Institut national pour l'évaluation et la sécurité de l'intelligence artificielle.

Si ce travail de refonte ou de projection conceptuelle est indispensable, il ne vaudra que par l'efficacité de sa mise en œuvre. A cet égard, il faut souligner les efforts produits par le SGDSN, toujours dans l'animation de la communauté interministérielle en associant nombre de partenaires extérieurs au monde de l'administration, pour publier des guides de sensibilisation permettant, sur des sujets d'importance, de diffuser largement l'information : le guide de résilience Tous responsables destiné à l'ensemble de la population ; plusieurs guides de sensibilisation aux ingérences numériques étrangères ; un aide-mémoire consacré à la résilience à destination des collectivités territoriales. On peut ajouter à cet ensemble l'important volume d'informations opérationnelles rendues publiques afin de dévoiler les attaques informationnelles et cyber subies par notre pays.

Si cet effort ne résume pas à lui seul l'intégralité des – nombreux – travaux menés et animés par le SGDSN dans ses différentes composantes, il concrétise à la fois la nécessité d'accélérer la préparation du pays et de notre population, rendue indispensable par la pression grandissante créée par les tensions internationales, et le caractère fondamentalement collectif des efforts à accomplir.

Ce rapport d'activité démontre à quel point ces objectifs guident le travail quotidien de chaque agent du SGDSN. Je vous en souhaite une bonne lecture. ◂

ORGANIGRAMME



Effectifs au 31 décembre 2025 (civils et militaires)

CABINET :	33
PSE :	63
AIST :	63
SAG :	115
ANSSI :	678
OSIIC :	294
VIGINUM :	64
HCEA :	8
GIC :	296

ÉLÉMENTS DE CHRONOLOGIE 2025

15 JANVIER
Entrée en vigueur de la posture Vigipirate « hiver-printemps 2025 »

13 FÉVRIER
Déplacement du secrétaire général, Stéphane Bouillon, à Bruxelles

28 FÉVRIER
Signature de l'amendement à l'Accord général de sécurité entre la France et le Portugal

23 JANVIER
Commission interministérielle de la sûreté aérienne

13 AU 18 MARS
Crisis Management Exercice (CMX) visant à entraîner au processus décisionnel le Conseil de l'Atlantique Nord et les autorités militaires de l'OTAN

26 MARS
Nicolas Roche est nommé secrétaire général de la défense et de la sécurité nationale

16 MAI
Déplacement du secrétaire général à Berlin

21 MAI
Lancement d'un nouveau programme interministériel classifié dont le pilotage est assuré par le SGDSN et la CNRLT

29 MAI
Déplacement du secrétaire général à Singapour, à l'occasion du Shangri-La Dialogue

29 MAI
Signature de l'accord général de sécurité avec Singapour

9 MAI
Déplacement du secrétaire général à Londres

5 JUIN
Commission interministérielle de défense et de sécurité des secteurs d'activités d'importance vitale (CIDS-SAIV)

19 JUIN
Comité de défense de zone Ouest à Rennes

3 JUIN
Déplacement du secrétaire général adjoint à Bagdad

23 JUIN
Comité interministérielle pour la résilience nationale

29 JUIN
Déclenchement de la CIC « canicule »

1ER JUILLET
Entrée en vigueur de la posture Vigipirate « été-automne 2025 »

9 JUILLET
Commission interministérielle de la sûreté aérienne

27 AOÛT
Xavier Brunetière est nommé Directeur de la Protection et de la sécurité de l'État

14 JUILLET
Publication de la Revue nationale stratégique 2025

5 AOÛT
Adaptation de la posture Vigipirate en réponse à l'attaque d'Israël sur l'Iran

4 SEPTEMBRE
Déplacement du Secrétaire général à l'OTAN - Bruxelles

9 SEPTEMBRE
Sébastien Lecornu est nommé Premier ministre

9 SEPTEMBRE
Déclenchement de la CIC « mouvement du 10 septembre »

C4

19 mars
28 avril
19 mai
16 juin
21 juillet
8 septembre
13 octobre
17 novembre
15 décembre

CIEEMG

16 janvier
6 février
13 mars
3 avril
15 mai
11 juin
3 juillet
4 septembre
9 octobre
13 novembre
4 décembre

CIA

27 janvier
1er juillet

10 SEPTEMBRE
Signature d'une convention de partenariat stratégique entre l'OSIIC et le MEAE

17 SEPTEMBRE
Déclenchement de la CIC « journée nationale d'actions du 18 septembre »

15 SEPTEMBRE
Déplacement du secrétaire général à l'UE - Bruxelles

4 OCTOBRE
Déplacement du secrétaire général adjoint à Singapour

6 AU 11 OCTOBRE
Déplacement du secrétaire général adjoint en Australie

14 AU 15 OCTOBRE
Exercice Hydros ayant pour vocation d'entraîner la cellule interministérielle de crise (CIC) à la gestion d'une crue de Seine, notamment sur le volet anticipation

14 OCTOBRE
Comité de zone de défense Est à Bure

10 OCTOBRE
Sébastien Lecornu est reconduit en tant que Premier ministre

7 OCTOBRE
Comité de défense de zone Nord à Lille

22 OCTOBRE
Publication de la feuille de route de transition et d'adaptation écologique du SGDSN

31 OCTOBRE
Fin de service de l'infrastructure de gestion de clés (IGC) THOT et entrée en service opérationnel de la nouvelle IGC permettant de gérer le cycle de vie des certificats numériques

13 NOVEMBRE
Signature de l'amendement à l'accord général de sécurité avec l'OCCAR (Organisation conjointe de coopération en matière d'armement)

27 NOVEMBRE
Séminaire handicap du SGDSN

3 DÉCEMBRE
Commission interministérielle de défense et de sécurité des secteurs d'activités d'importance vitale (CIDS-SAIV)

15 DÉCEMBRE
Déclenchement de la CIC « crise agricole »

17 DÉCEMBRE
Commission interministérielle de sûreté aérienne

19 DÉCEMBRE
Inauguration des nouveaux modulaires situés sur le site de l'HNI

15 DÉCEMBRE
Déplacement du secrétaire général à Rome

COLMI

12 février
16 avril
27 mai
25 juin
1 octobre

CIBDU

15 janvier
5 février
12 mars
2 avril
15 mai
11 juin
2 juillet
30 juillet
3 décembre

COLISÉ

10 février
18 avril
20 juin
23 juillet
15 octobre
10 décembre

10

RNS 2025

ACTUALISATION DE LA REVUE NATIONALE STRATÉGIQUE

« Nous sommes à un point de bascule. ».

Emmanuel Macron,
Revue nationale de stratégie 2025

Le 14 juillet a été publiée l'actualisation de la Revue nationale stratégique (RNS 2025). Cette actualisation, commandée par le Président de la République lors de ses vœux aux armées le 20 janvier complète les travaux réalisés en 2022, en préparation de ceux sur la loi de programmation militaire 2024-2030. Elle propose les actions nécessaires pour que notre défense s'adapte à un nouvel environnement dégradé et définit les contours de la défense globale du pays et du réarmement, y compris moral, de la Nation. Organisés par le SGDSN, les travaux ont largement associé l'ensemble des ministères. À la demande du Président de la République et du Premier ministre, un effort particulier a été fait en matière de consultation des commissions parlementaires en charge de la défense, de la délégation parlementaire au renseignement et des associations d'élus régionaux, départementaux et locaux. Le monde de la recherche et des groupes de réflexion ont aussi été associés. Ces travaux, menés du mois de février au mois de juin, sont présentés dans un document en trois parties qui fixe l'ambition de la France en matière de défense et de sécurité nationale à l'horizon 2030.

— LE CONTEXTE STRATÉGIQUE EN 2025

D'ici 2030, la principale menace pour la France et les pays européens est désormais celle d'une guerre ouverte contre le cœur de l'Europe, impliquant un engagement majeur de nos armées en dehors du territoire national qui s'accompagnerait, en parallèle, d'une augmentation massive des attaques hybrides sur notre sol et contre nos intérêts dans le monde. La RNS 2025 prend en compte ce contexte : la France et ses partenaires européens doivent être capables de mieux se défendre et de dissuader la Russie de mener une nouvelle agression sur le continent. La RNS 2025 présente une approche de défense et de sécurité nationale globale qui mobilise l'État dans son ensemble et implique toute la Nation. De façon préventive, il convient de parer aux vulnérabilités d'approvisionnement en procédant à la recension des biens vitaux et en mitigeant les risques liés aux importations les plus stratégiques par la diversification des sources d'approvisionnement, éventuellement la relocalisation de certaines productions, la sécurisation juridique des contrats d'approvisionnement, voire la constitution de réserves stratégiques.

— UNE AMBITION 2030 ACTUALISÉE

Dans la RNS 2025, la France affiche son ambition d'être armée matériellement et moralement en 2030, pour faire face et gagner, avec ses alliés et partenaires, une guerre majeure de haute intensité dans le cœur de l'Europe. Elle est également en mesure de gérer les conséquences d'actions déstabilisatrices qui se produiront sur le territoire national. Pour ce faire, grâce à son modèle d'armée, ses capacités d'action et d'influence souveraines, la France agit selon quatre priorités :

- défendre l'Europe, y compris par sa dissuasion nucléaire
- garantir sa sécurité, la défense de ses intérêts et celle de ses alliés extra-européens dans le cadre de partenariats renouvelés
- protéger et défendre le territoire national, la population et les ressortissants français
- contribuer à la stabilité de la région indopacifique

— ONZE OBJECTIFS STRATÉGIQUES ISSUS DE CETTE AMBITION

Le premier objectif stratégique est de disposer d'une dissuasion nucléaire crédible, indépendante et souveraine, clé de voûte de notre politique de défense.

Comme deuxième objectif, la France entend garantir sa résilience, dans l'Hexagone comme en outre-mer. Elle doit pouvoir faire face de manière simultanée, à des crises et à des actions hybrides adverses sur le théâtre national.

Le développement d'une économie qui se prépare à la guerre constitue le troisième objectif stratégique.

Le quatrième objectif est la pérennisation de la présence française dans le premier cercle des puissances cyber.

Le cinquième objectif est d'assumer notre rôle d'allié fiable au profit de la défense de l'Europe, en particulier face à la Russie dans le cadre d'un pilier européen renforcé et rééquilibré de l'Alliance atlantique.

La France a pour sixième objectif de contribuer à un réel changement d'échelle pour le renforcement des capacités européennes de défense dans les domaines technologique, capacitaire, opérationnel et en termes de résilience de l'Europe, en particulier au plan énergétique.

La France doit également approfondir et diversifier ses coopérations internationales. Il s'agit de développer une nouvelle offre partenariale en Afrique, de consolider notre engagement au Proche et Moyen-Orient, de contribuer à la sûreté des espaces communs et à la stabilité régionale en Méditerranée et en mer Rouge, et de renforcer les coopérations en Indopacifique. L'intégration et la place des territoires ultramarins français seront renforcées à ce titre dans les partenariats régionaux.

La France entend concentrer ses efforts pour disposer d'une autonomie d'appréciation et une souveraineté décisionnelle garanties. Ce huitième objectif stratégique nécessite de renforcer les capacités de renseignement et d'action de l'État.

La capacité à agir dans les champs hybrides (cyberespace, sphère informationnelle, droit et économie, opérations militaires) constitue le neuvième objectif stratégique.

Dixième objectif stratégique, la France doit disposer des capacités militaires pour préserver sa liberté d'action et défendre ses intérêts en toute circonstance.

Face à l'accélération des développements scientifiques et technologiques et leur utilisation généralisée par ses compétiteurs et ses adversaires, la France doit disposer d'une excellence académique, scientifique et technologique au service de la souveraineté française et européenne. Ce onzième et dernier objectif stratégique est une évolution majeure de l'actualisation de la Revue nationale stratégique.

L'atteinte de l'ambition 2030 dans le contexte décrit passera par une augmentation des budgets pour accélérer le réarmement de la France et pivoter résolument vers une Nation plus résiliente, prête à faire face à une guerre de haute intensité.

14

FAIRE FACE À DES MENACES NOUVELLES

PLANIFIER

— 2025 : UN CADRE STRATÉGIQUE RENOUVELÉ AU SERVICE DE LA RÉSILIENCE NATIONALE

En 2025, la sous-direction sécurité et résilience nationales - SRN, anciennement PSN - a continué son travail dans un cadre doctrinal renouvelé par l'actualisation de la Revue nationale stratégique publiée le 14 juillet (RNS 2025), dressant le constat de menaces plus pressantes et assignant au pays, en réponse, l'ambition d'une meilleure résilience, une préparation résolue à des crises de haute intensité et l'adaptation de l'ensemble de nos travaux de planification aux nouvelles menaces.

RENFORCER LA RÉSILIENCE DE LA NATION

L'année 2025 marque une évolution majeure de la Stratégie nationale de résilience qui connaît un recentrage, en cohérence avec les ambitions de la RNS - notamment de son objectif stratégique numéro 2 Une France unie et résiliente-. Le 23 juin 2025, le Comité interministériel pour la résilience nationale a entériné la restructuration de la SNR autour de deux priorités et de 11 actions opérationnelles, associées à un calendrier.

La première priorité est d'assurer la continuité économique de la vie de la Nation. Il s'agit donc de garantir le fonctionnement des réseaux essentiels, parmi lesquels les numéros téléphoniques d'urgence, les communications de l'État, les approvisionnements en eau et en énergie et les services numériques. De façon préventive, il convient de parer aux vulnérabilités d'approvisionnement en procédant à la recension des biens vitaux et en mitigeant les risques liés aux importations les plus stratégiques par la diversification des sources d'approvisionnement, éventuellement la relocalisation de certaines productions, la sécurisation juridique des contrats d'approvisionnement, voire la constitution de réserves stratégiques.

La seconde priorité est de mobiliser l'ensemble des citoyens au service de la résilience de la Nation. Cette mobilisation passe par l'éducation et la formation aux risques majeurs à tous les âges et sur l'ensemble du territoire national. À cette fin, plusieurs vecteurs sont utilisés, comme le guide Tous Responsables, une communication publique régulière, l'introduction d'une pédagogie de la résilience dans les programmes scolaires et la promotion d'une résilience territoriale. Parallèlement, un vivier de compétences mobilisables en cas de crise doit être créé. Ce qui passe par une profonde réforme des systèmes actuels de réserve.

En complément à cette restructuration de la SNR, le directeur de cabinet du Premier ministre a souhaité disposer d'un projet de refonte de la structuration des réserves et d'un Plan de défense et de sécurité nationale qui accompagnera la montée en puissance de la Nation aux côtés des armées, en cohérence avec l'hypothèse structurante d'un engagement militaire majeur tel que décrit dans la Revue nationale stratégique.

RENFORCER LA PROTECTION DES INFRASTRUCTURES ET ENTITÉS CRITIQUES

La poursuite de la transposition de la directive européenne (UE) 2022/2557 sur la résilience des entités critiques a fortement mobilisé la direction de la protection et de la sécurité de l'État. Les travaux ont progressé dans plusieurs directions. Il s'est notamment avéré indispensable de vérifier la cohérence entre le dispositif national et le nouveau cadre. Les ministères et les acteurs concernés ont été accompagnés dans leur prise en compte des nouvelles exigences. L'articulation entre la réalité des besoins et les moyens a été mesurée au plus juste. L'ensemble de ces travaux préparatoires a permis d'aboutir à un projet de loi pertinent et réaliste. Une fois votée, la loi permettra de passer d'une logique de protection physique à une logique de continuité d'activité des opérateurs, en s'appuyant sur l'analyse préalable des dépendances. Le régime des sanctions sera modernisé et simplifié. Les possibilités de recours aux enquêtes administratives de sécurité seront élargies. Dans l'attente de l'entrée en vigueur des nouvelles dispositions, la direction de la protection et de la sécurité de l'État veille, aux côtés des services ministériels des hauts fonctionnaires de défense et de sécurité, à ce que les opérateurs s'alignent progressivement et par anticipation sur les exigences de la directive, sur une base incitative fondée sur une perception commune de l'urgence de s'adapter à un contexte qui évolue rapidement.

ACCÉLÉRER LA PRÉPARATION DES TERRITOIRES

Des contacts étroits et fréquents ont été maintenus avec les associations d'élus et de dirigeants territoriaux, ainsi que les associations agréées de sécurité civile. La Revue nationale stratégique et la stratégie nationale de résilience ont fait l'objet de réunions spéciales de concertation préalable, puis de présentation, avec les directeurs généraux d'associations d'élus et de responsables administratifs territoriaux ou leur représentant. Par ailleurs, le centre national de la fonction publique territoriale a complété son offre de formation en ligne sur la déclinaison locale de la SNR par la mise en ligne d'un cours à la fin du mois de septembre. A la fin de l'année 2025, ce MOOC avait été suivi par près de 5 000 personnes. De plus, un travail d'actualisation du site destiné aux élus est en cours. Il est mené avec le CNED et les associations partenaires. Sa mise en ligne doit intervenir au printemps 2026. Au sein de l'administration de l'État, la direction générale de l'administration et de la fonction publique (DGAFP) a confirmé sa volonté d'ouvrir un espace consacré à la résilience des services publics, à l'intention des cadres de l'administration afin de compléter sous l'angle managérial les formations d'ores et déjà disponibles pour tous les agents sur la plate-forme de formation Mentor. Enfin, six associations de cadres dirigeants territoriaux, réunis dans un groupe de travail co-animé par le SGDSN et le centre d'études et d'expertise sur les risques, l'environnement, la mobilité et l'aménagement, Cerema, ont produit un recueil contenant une première série de fiches de « bonnes pratiques » à destination des collectivités territoriales.

LE GUIDE TOUS RESPONSABLES

La diffusion d'un guide[1] destiné à la population est l'une des 11 actions de la SNR recentrée. Publié le 20 novembre, soit 5 mois après l'entrée en vigueur de la nouvelle version de la Stratégie, ce guide est l'un des outils de renforcement de la préparation de la Nation.

Conçu comme un manuel de référence, il propose des gestes et des repères essentiels à connaître en cas de crise, des actions à entreprendre dès à présent pour mieux s'en prémunir, et présente différents moyens de s'engager au service de la collectivité. En quelques pages, chacun peut ainsi mieux s'informer sur les risques et les menaces, sur ce qu'il convient de préparer dans son kit d'urgence, sur les formations aux gestes de premiers secours, *etc.*

La Directive générale interministérielle n °320 définit 5 typologies de menaces et 3 typologies de risques.

MENACES

- menace extérieure, agression
- attentats, de nature NRBC ou non (terrorisme, tuerie de masse, prise d'otages...)
- troubles sociétaux graves (violences urbaines, migrations massives...)
- cyber
- hybrides

RISQUES

- naturels
- technologiques ou industriels
- sanitaires

[1] Disponible sur le site du SGDSN : https://www.sgdsn.gouv.fr/publications/guide-tous-responsables

ENTRAÎNER, FORMER, PLANIFIER, TESTER

Garante de l'organisation de gestion des crises majeures pour le Premier ministre, la direction de la protection et de la sécurité de l'État a assuré sa mission de préparation de la réponse de la Nation, par la formation des agents de la fonction publique ou la mise en place d'exercices interministériels majeurs.

L'année 2025 aura été l'occasion d'une refonte de la cartographie des formations, d'une redynamisation des groupes de réflexions interministériels, de la diversification des exercices proposés et d'une actualisation des outils de gestion de crise. Ces travaux permettront à l'avenir la constitution d'un vaste réseau d'acteurs rapidement déployable, formés à la gestion de crise et aptes à assurer efficacement la résilience de la Nation en cas d'événement majeur.

S'ADAPTER AUX NOUVEAUX DÉFIS DE LA LUTTE ANTI-DRONES

L'année 2025 marque une accélération significative des efforts interministériels en matière de lutte anti-drones, coordonnés par la Commission interministérielle de la sûreté aérienne (CISA). Avec pour objectif principal d'accélérer les efforts engagés depuis une dizaine d'années, une feuille de route interministérielle a été proposée par le SGDSN et approuvée par le cabinet du Premier ministre au mois de juillet. Sa mise en œuvre a débuté aussitôt. Parallèlement, un centre d'essais et de tests a été lancé pour permettre une émergence plus rapide de solutions technologiques de détection et de neutralisation des drones pirates, adaptées au secteur civil, notamment privé.

CHIFFRES CLEFS DE L'ANNÉE 2025

1 300 agents formés à la planification et la gestion de crise depuis 2019, dont 212 nouveaux en 2025

4 exercices gouvernementaux

5 expérimentations en situation réelle de technologies d'avenir en matière de sécurité

500 chiens formés à la détection d'explosifs

11 actions dans la Stratégie nationale de résilience recentrée

18

— ACCÉLÉRER L'INNOVATION TECHNOLOGIQUE POUR LA RÉSILIENCE NATIONALE

Les enjeux capacitaires de la SNR pour les technologies de sécurité et de résilience ont conduit en 2025 à engager trois axes d'efforts : anticiper l'apport des technologies pour la résilience des entités critiques ; développer les outils adaptés de gestion de crise aux collectivités territoriales ; renforcer la résilience des réseaux. Une large consultation des acteurs et de leurs besoins a abouti à sept expérimentations de solutions technologiques en conditions réelles, traitant de l'anticipation et la gestion des submersions marines, la résilience des réseaux à l'échelle d'une métropole ou la lutte anti-drones adaptée aux besoins de protection des points d'importance vitale. Ces expérimentations, débutées en 2025, sont aussi la préfiguration d'une démarche de labélisation et de certification des solutions techniques qui seraient retenues afin d'inciter les acteurs publics et privés à se doter de technologies de confiance souveraines.

De surcroît, ces expérimentations contribuent au renforcement de la base industrielle et technique de sécurité, qui est l'un des objectifs de la RNS. En la matière, le SGDSN a poursuivi ses actions de soutien à la filière des industries de sécurité, notamment en matière de recherche et d'innovation et a conclu une nouvelle convention avec l'Institut national de recherche en sciences et technologies du numérique, INRIA, sur les apports de l'intelligence artificielle à la sécurité. Sur le plan européen, une attention particulière a été accordée à l'accès aux financements de recherche et innovation de sécurité, dans le cadre du volet politique industrielle de résilience et de sécurité du futur fonds européen de compétitivité de la Commission européenne.

— PRÉPARATION, FORMATION ET COORDINATION FACE AUX RISQUES NRBC

Dans un contexte d'instabilité géopolitique, la menace nucléaire, radiologique, biologique et chimique (NRBC), jusqu'à présent de nature terroriste, comprend désormais les menaces d'origine étatique. Si ni les modes opératoires, ni les capacités de réponse ne sont directement affectés, notre capacité collective à reconnaitre un événement NRBC touchant un faible nombre de victimes, voire une seule victime, doit être renforcée en développant notre vigilance et notre capacité de détection précoce.
L'année 2025 a vu le renforcement de la formation des acteurs du domaine grâce aux actions du centre national civil et militaire de formation et d'entraînement NRBC-E d'Aix-en-Provence, en lien avec le SGDSN. Ainsi, les intervenants de la sécurité civile, de la santé et des forces de sécurité intérieure ont été sensibilisés aux spécificités de la prise en charge des enfants en situation NRBC *via* un webinaire spécialisé et des entrainements dispensés au sein des centres d'entrainement zonaux.

La cellule interministérielle spécialisée en décontamination des infrastructures a réalisé un exercice afin d'améliorer les échanges entre experts des différents ministères. Cet exercice a permis de tester les capacités de la Cellule interministérielle spécialisée en décontamination d'infrastructures à produire des éléments d'arbitrage pour la cellule interministérielle de crise.

Les 26 et 27 novembre, le réseau national des laboratoires BIOTOX-PIRATOX-PIRATOME a réuni pas moins de 180 personnes au Val-de-Grâce lors de son séminaire annuel et a permis d'assurer la cohésion des différents laboratoires du réseau autour de thèmes peu abordés dans leurs pratiques habituelles.

Enfin, il est à noter l'obtention d'une autorisation d'accès précoce accordée par les autorités sanitaires pour le Ricimed®, seul antidote existant contre les intoxications à la ricine – première mondiale conjointement impulsée par le SGDSN et la direction générale de l'armement et développé par une entreprise française –. Cette autorisation a depuis lors été remplacée par une autorisation de mise sur le marché délivrée le 12 janvier 2026.

— POURSUIVRE LA RÉFORME DE LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE AUX NIVEAUX NATIONAL ET INTERNATIONAL

Garante de la protection du secret de la défense nationale, la direction de la protection et de la sécurité de l'État a maintenu ses efforts tant au niveau national qu'international pour promouvoir cette politique indispensable à la protection des intérêts fondamentaux de la Nation.

En 2025, la direction a renforcé l'animation de son réseau de fonctionnaires de sécurité de défense (FSD) placés auprès de chaque haut fonctionnaire de défense et de sécurité des ministères, réunis une fois par trimestre, et l'animation semestrielle des correspondants du réseau national OTAN et UE.

Elle a également poursuivi l'accompagnement des ministères dans la déclinaison de l'IGI 1300. La direction a continué ses travaux d'élaboration d'un parcours numérique à destination des personnes habilitées afin de les former et les sensibiliser à certains aspects de la politique de protection du secret de la défense nationale.

Par ailleurs, elle a piloté, en lien avec l'OSIIC, des travaux visant à dématérialiser la procédure, la gestion et le suivi des habilitations au secret de la défense nationale, afin d'en accélérer et d'en sécuriser le traitement. Ces travaux se poursuivront en 2026 avec, en particulier, la mise en place d'une équipe de projet interministérielle, pilotée par la direction, et la réalisation d'ateliers « métiers » avec les différents ministères, afin de mettre en place de nouveaux outils numériques.

La direction a poursuivi et accentué sa mission de contrôle de l'application de la réglementation nationale, européenne et otanienne et du niveau de protection des informations les plus sensibles. Sept missions d'inspection ont ainsi été menées en 2025.

Sur le plan international, la direction a accéléré ses travaux de révision des accords généraux de sécurité (AGS) en lien étroit avec les acteurs interministériels (MINARM et MEAE en particulier). L'année 2025 a été marquée par la signature d'un AGS avec le Portugal et Singapour. Elle a également été l'occasion de la signature de la révision de l'Accord de sécurité de l'Organisation conjointe de coopération en matière d'armement (OCCAR) à Paris le 13 novembre 2025. Des négociations actives sont par ailleurs conduites en parallèle avec plusieurs pays : Allemagne ; Italie ; Royaume-Uni ; Pays-Bas ; Inde ; Ukraine ; Canada.

CHIFFRES CLEFS DE L'ANNÉE 2025

25 participations à des comités de sécurité en tant qu'autorité nationale de sécurité

6 420 décisions d'habilitation délivrées par la sous-direction de la protection du secret de la défense nationale dans son périmètre de compétence

4 réunions des FSD

3 AGS signés

7 inspections menées en France au titre de la protection des informations ou de supports classifiés au niveau Très Secret faisant l'objet de classifications spéciales, de l'OTAN et de l'UE

XAVIER **BRUNETIÈRE**

Préfet, Directeur de la Protection
et de la Sécurité de l'État

« Notre boussole est le scénario central de la RNS »

L'actualisation de la Revue nationale stratégique (RNS) menée en 2025 a accordé une place prépondérante à la résilience. Quelles sont les conséquences concrètes pour PSE ?

Cette actualisation pose le diagnostic d'un monde plus dangereux, plus incertain où les risques et les menaces s'accroissent et constituent autant de défis face auxquels nous devons nous préparer. En la matière, notre boussole est le scénario central de la RNS : un engagement majeur de nos forces armées aux frontières de l'Europe ; la nécessité de faire face à une forte hausse des attaques hybrides sur le territoire national ; un effort à fournir de l'ensemble des secteurs d'activité pour maintenir leur activité et soutenir les forces armées, tout en pouvant faire face à des crises intérieures d'ampleur. Pour la direction de la protection et de la sécurité de l'État, l'atteinte des objectifs induits par ce scénario central se résume simplement : coordonner la préparation des aspects civilo-militaires et adapter notre rythme pour être au rendez-vous des premières échéances, en 2030.
Concrètement, nous avons recentré la Stratégie nationale de résilience de 2022 autour de deux priorités : la continuité de la vie économique de la Nation et la mobilisation de la population en comptant sur l'esprit d'engagement des citoyens. Nous avons également accéléré le rythme des exercices interministériels, intensifié le dialogue civilo-militaire, poursuivi la réforme de la planification de sécurité nationale - par exemple en rénovant le plan Vigipirate -, accompagné nos opérateurs d'importance vitale dans la déclinaison de la directive sur la Résilience des entités critiques (REC), développé nos partenariats avec les collectivités territoriales.
Nous contribuons également aux travaux de deux mandats spécifiques. Le premier, piloté par le capitaine de vaisseau(R) Lallement, vise à élaborer un plan de défense et de sécurité nationale visant à garantir le fonctionnement de l'État et la résilience de la Nation en intégrant les contraintes liées au scénario central de la RNS. Il s'agit de définir un catalogue de mesures, des contrats opérationnels déclinés par ministère et un niveau d'alerte publique pour rendre compte de la posture générale. Le deuxième, piloté par Mme Dumas, vise à cartographier, organiser et sincériser les divers viviers de réserves puis de diffuser un guide pour valoriser l'engagement et simplifier les modalités pratiques d'un parcours usager.

Au plan international, nous relevons aussi notre niveau d'exigence pour renforcer la coordination avec nos alliés et les États membres de l'UE, tout en démontrant notre solidarité stratégique dans les cadres multilatéraux – en particulier à l'OTAN et à l'UE – comme bilatéraux.
Conformément aux orientations du secrétaire général, notre organisation s'adapte afin d'être plus agile et plus lisible.

La direction PSE s'est aussi transformée en 2025.

C'est exact. L'année 2025 aura conforté la direction de la protection et de la sécurité de l'État dans ses missions : garantir la continuité de l'action gouvernementale, renforcer la préparation de l'État face aux crises majeures et assurer la protection du secret de la défense nationale. Dans un environnement marqué par l'accélération des crises, l'augmentation des risques de tous ordres et par le durcissement de certaines menaces stratégiques, la direction PSE a poursuivi un double objectif : mieux anticiper, en consolidant nos outils de planification ▸▸▸

et de compréhension des risques et des menaces ; mieux résister, en renforçant la résilience nationale, la robustesse des acteurs essentiels et la protection des informations sensibles. Préparée au long de l'année 2025 et effective depuis le 1er décembre, notre nouvelle organisation est plus agile et moins cloisonnée. Ainsi, l'ancienne sous-direction de la planification de sécurité nationale est devenue la sous-direction de la sécurité et de la résilience nationales (SDSRN), structurée autour d'une mission des affaires internationales et de deux pôles calqués sur les différentes phases d'une crise et de sa gestion : résilience et sûreté des milieux, d'une part, et préparation et réponse aux crises, d'autre part. Ce choix assure une approche transversale, sans angle mort, en assurant la cohérence de notre action au service de la préparation du pays. De la sorte, nous nous articulons aussi plus aisément avec les autres services du SGDSN et avec nos interlocuteurs permanents comme les services des hauts fonctionnaires de défense et de sécurité des ministères.

En matière de résilience, comment passe-t-on du concept à la réalité ?

En la matière, le concept est plus simple à appréhender qu'à mettre en œuvre. Il s'agit d'être capable, tout à la fois, de tenir sans céder, d'absorber des chocs successifs, d'assurer la continuité de l'action de l'État et des opérateurs les plus vitaux dans des conditions dégradées – voire très dégradées – face à une myriade de perturbations possibles et, *in fine*, d'assurer le retour à la normale. C'est vaste ! Pour y parvenir, notre méthode implique trois étapes. D'abord, travailler en amont à partir du réel : comprendre les risques et les menaces, anticiper les signaux faibles et analyser les vulnérabilités, les dépendances en matière d'énergie, de télécommunications, de données informatiques, de logistique… Sans cet effort, il n'est pas possible de détecter les points de rupture, d'identifier les capacités nécessaires ou de générer les ressources humaines. De surcroît, ces travaux nécessitent du temps et la mise en œuvre des conclusions encore plus !
Ensuite, s'entraîner : les exercices, à partir de scénarios exigeants, servent à révéler les fragilités et à y remédier, dans une logique de retour d'expérience permanent. Enfin, outiller : des documents courts, des réflexes partagés, des chaînes d'alerte et des fiches de mesures claires à mettre en oeuvre, et des exigences compréhensibles. Le but est que chaque acteur, public comme privé, puisse répondre sans hésiter aux questions *Que maintenir en priorité ? Avec quels moyens ? Comment revenir à un fonctionnement normal ou acceptable ?* C'est un mouvement d'ensemble, car la résilience d'une Nation est celle de chacune de ses composantes, et réciproquement. Thucydide l'exprimait déjà : « *La force de la cité ne réside ni dans ses remparts, ni dans ses vaisseaux, mais dans le caractère de ses citoyens.* ». En 2025, nous avons par exemple produit, à l'instar de nos partenaires européens, le guide Tous responsables, qui expose les risques et menaces et fournit des conseils sur les manières de réagir. C'est aussi le sens de la directive *Résilience des entités critiques* - REC qui permet aux opérateurs d'importance vitale d'avoir une planification intégrant la protection contre les actes de malveillance et la continuité d'activité. La finalité est la même : assurer la continuité de l'État et la robustesse de la Nation, quoi qu'il arrive. ◂

2

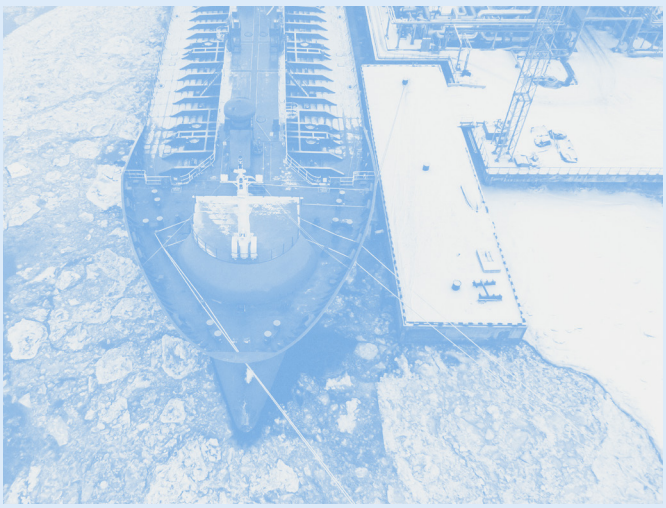
CONSOLIDER LA POSITION INTERMINISTÉRIELLE

COOPERER

— ACTION INTERNATIONALE

A raison de ses missions, de sa vision globale des questions de sécurité et de défense et de sa place dans l'appareil d'État, le SGDSN est un interlocuteur privilégié pour nos partenaires internationaux, notamment lorsqu'ils sont dotés d'une organisation comparable. En 2025, dans un contexte géopolitique particulièrement dégradé et incertain, le SGDSN a poursuivi le renforcement de dialogues bilatéraux en particulier avec Singapour, l'Australie, l'Inde, le Japon, le Qatar et le Royaume-Uni, partenaires plus que jamais essentiels. Le SGDSN, avec la direction AIST, a également été engagé au sein d'instances multinationales (UE, OTAN) ainsi que dans différents *fora* dans lesquels il porte la position française. Par ailleurs, la direction AIST concourt à l'élaboration et au suivi de la mise en œuvre de stratégies interministérielles à dimension internationale répondant aux enjeux de souveraineté et de protection des intérêts nationaux. Ce fut le cas, avec le ministère de l'Europe et des affaires étrangères, pour la stratégie Indopacifique, dont la nouvelle version a été diffusée le 18 juillet 2025.

— MENACES HYBRIDES



En 2025, nos adversaires ont intensifié l'usage de stratégies hybrides contre les pays européens : sabotages ; ingérences numériques étrangères, notamment en période électorale ; cyberattaques ; atteintes à notre sécurité économique ; survols de drones pirates, *etc.*

La prise de conscience générale de cette menace croissante se poursuit, ainsi que le développement d'une organisation nationale toujours plus robuste. Dans ce cadre, le groupe de travail (GT) interministériel permanent piloté par la direction AIST a concentré ses efforts sur le développement d'une vision consolidée des signalements, analyses et réponses des services opérant dans ces différents champs hybrides. C'est dans cette optique que le GT a pu travailler en 2025 sur une revue des actions hybrides en lien avec la guerre en Ukraine, a contribué aux travaux sur les mécanismes d'entrave à la flotte fantôme russe, a travaillé à l'élaboration d'une doctrine nationale de lutte contre les menaces hybrides et a engagé des travaux de recension des ingérences étrangères contre la France.

Au-delà de ce seul GT, le SGDSN mène un dialogue nourri sur la question des menaces hybrides avec nos alliés et partenaires, aussi bien dans les formats multilatéraux de l'UE et de l'OTAN que bilatéraux. Ainsi, en 2025, le SGDSN a organisé ou participé à une quarantaine d'échanges ou événements internationaux consacrés à la lutte contre les menaces hybrides. Enfin, AIST assure l'interface entre l'interministériel et la cellule de fusion hybride du centre de situation et de renseignement de l'UE. Elle représente également la France au sein du centre d'excellence d'Helsinki (*CoE*) sur les menaces hybrides, qui rassemblait, depuis 2024, l'ensemble des membres de l'UE et de l'OTAN, à l'exception des État-Unis d'Amérique qui s'en sont retirés en janvier 2026.

LES DISPOSITIFS NATIONAUX DE GELS DE BIENS ET D'AVOIRS

Dans le cadre de la lutte contre le financement du terrorisme le SGDSN a assuré le secrétariat du groupe de travail interministériel sur le gel des avoirs à but antiterroriste (GABAT). Au 12 décembre 2025, 476 mesures de gel des avoirs pour motif de terrorisme étaient en vigueur sur le territoire national. Le GABAT, qui regroupe l'ensemble des services et des ministères compétents, s'assure de la bonne circulation de l'information. Il simplifie ainsi le recours au mécanisme des gels d'avoirs visant la menace terroriste. Les mesures de gel ont été multipliées par dix depuis la création du groupe en 2017. Le SGDSN organise et rend compte des séances de travail.

Sur le modèle du GABAT, la loi du 25 juillet 2024 visant à prévenir les ingérences étrangères en France a créé un dispositif de gels d'avoirs et de biens en lien avec l'ingérence étrangère (GABIN). AIST a participé, en 2025, aux travaux de préfiguration et d'opérationnalisation de ce dispositif, dont le SGDSN assure le secrétariat avec la CNRLT.

— EXPORTATIONS DE MATÉRIELS DE GUERRE (EMG)

Le SGDSN assure le contrôle des exportations des matériels de guerre et préside à ce titre la Commission interministérielle pour l'étude des exportations des matériels de guerre (CIEEMG), qui comprend en outre les ministères chargés des affaires étrangères, des armées et de l'économie. Dans le droit national, l'exportation, des matériels de guerre est interdite. Toute opération d'exportation constitue donc une dérogation au principe général d'interdiction, accordée au cas par cas. Cette dérogation prend la forme d'une licence d'exportation octroyée par le Premier ministre, après avis de la CIEEMG. Par délégation du Premier ministre, la licence peut être accordée par le SGDSN. Une session plénière de la CIEEMG est organisée chaque mois, afin de débattre des dossiers qui appellent un examen approfondi. Les dossiers les plus sensibles sont ensuite présentés à la décision du Premier ministre ou de son cabinet. En 2025, le nombre de licences déposées par les exportateurs a augmenté de près de 11 % par rapport à l'année 2024 avec un total de plus de 13 420. La CIEEMG a instruit près de 8 000 demandes de licences d'exportation recevables dont près de la moitié portent sur des modifications ou des prorogations de licences existantes. Ce chiffre témoigne du niveau élevé des projets d'exportation des industriels français de la défense, dans la continuité de l'activité observée depuis 2022.

En 2025, les membres de la CIEEMG ont été encore particulièrement mobilisés dans le traitement des licences au profit de l'Ukraine. Ces licences, traitées dans le strict respect des processus établis en matière de contrôle des exportations, ont fait l'objet d'un traitement accéléré, afin de répondre au besoin opérationnel des armées ukrainiennes, dans les meilleurs délais.

Parallèlement, le SGDSN coordonne des travaux réglementaires au niveau national au sein d'un comité technique annuel ou biannuel qu'il préside. Dans la continuité de la parution du guide sur le traitement des exportations de biens dits intangibles, le SGDSN a également poursuivi ses travaux pour mieux encadrer les nouvelles pratiques numériques et le travail nomade, qui créent de nouveaux enjeux en matière de contrôle des exportations. Ces travaux devraient aboutir au cours de l'année 2026.

Au plan international, la direction AIST entretient des échanges avec ses partenaires, dans le cadre de dialogues bilatéraux, des réunions du groupe de la *Letter of Intent* et de l'Accord sur les exportations en matière de défense, dont les travaux d'élargissement se poursuivent.

Enfin au plan européen, le SGDSN a été directement associé aux travaux menés dans le cadre de la révision de la Position commune et à la contribution française aux différents instruments mis en place par la Commission européenne dans le cadre du plan *Rearm Europe*. En lien avec le SGAE, le SGDSN a fait valoir ses positions sur la préservation de notre souveraineté en matière de contrôle des exportations et sur la préférence européenne.

Sur le volet financier, AIST a participé à la conférence consacrée au financement de la BITD, organisée par le ministère de l'économie le 20 mars 2025. A cette occasion, un dialogue de place co-présidé par M. Hervé Guillou et M. Philippe Brassac a pu être lancé. Il s'agit notamment de lever les freins structurels au financement du secteur de la défense, de renforcer la mobilisation de l'épargne privée et de faire émerger des propositions opérationnelles, dans une logique de souveraineté et de compétitivité. Dans la continuité de ce dialogue, AIST devrait en 2026 participer à des séances d'information au profit de la place financière, afin de sensibiliser ses acteurs sur le processus de contrôle export mis en place au travers de la CIEEMG.

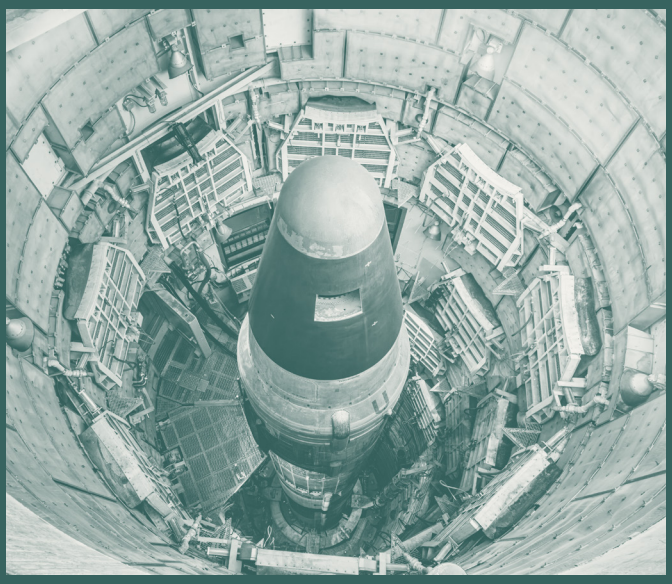
ACCORD SUR LES EXPORTATIONS DANS LE DOMAINE DE LA DÉFENSE

Depuis 2021, les industriels français, allemands et espagnols bénéficient de l'Accord sur les exportations en matière de défense qui vise à favoriser le développement de coopérations entre les industries de défense des États parties, ainsi qu'à rendre les procédures d'autorisation plus efficaces. Cet accord découle de celui passé entre la France et l'Allemagne en 2019.

L'année 2025 a été marquée par l'élargissement de cet Accord, dont la France est l'État dépositaire. Le Royaume-Uni a officiellement rejoint l'Accord le 5 décembre 2025. Les Pays-Bas devraient prochainement confirmer leur adhésion, dès que le processus interne de ratification aura été mené à son terme au cours de l'année 2026. La candidature italienne, en cours d'examen par les États parties, devrait être abordée fin février 2026 à l'occasion de la réunion du Comité permanent à Madrid. Enfin, la Suède a fait acte de candidature à l'automne 2025. Le SGDSN a eu un rôle actif dans ces travaux d'élargissement et a accueilli le comité permanent de l'Accord en juin 2025.

— LUTTE CONTRE LA PROLIFÉRATION DES ARMES DE DESTRUCTION MASSIVE : UN FIL CONDUCTEUR DE L'ACTION DE LA DIRECTION AIST

Le SGDSN assure un rôle de coordination dans la lutte contre la prolifération des armes de destruction massive (ADM) et de leurs vecteurs. Cette lutte s'exerce au travers d'actions transversales telles que le contrôle des exportations de biens à double usage (BDU), la participation aux régimes définissant les biens sensibles à contrôler ou la protection du potentiel scientifique et technique de la nation (PPST). Pour ce faire, le SGDSN doit avoir une vision précise et actualisée des risques de prolifération et être en capacité de caractériser les menaces liées aux agents nucléaires, radiologiques, biologiques, chimiques et explosifs (NRBCE). A ces fins, la direction AIST pilote l'élaboration d'analyses interministérielles sur des dossiers sensibles et sur des technologies innovantes ou de rupture comme la fabrication additive, la biologie de synthèse et, depuis 2025, sur l'intelligence artificielle. De plus, le SGDSN suit l'impact de la détérioration des relations internationales sur le fonctionnement des traités et des dispositifs de lutte contre la prolifération.



— EXPORTATIONS DE BIENS À DOUBLE USAGE (BDU)

Le SGDSN préside la commission interministérielle des biens à double usage (CIBDU), dont le secrétariat est assuré par le service des biens à double usage, qui relève du ministère chargé de l'industrie. Dans ce cadre, AIST contribue au contrôle des exportations de biens et technologies à finalité duale susceptibles d'avoir une utilisation tant civile que militaire, ainsi qu'à la mise en œuvre des sanctions visant certains pays. Elle organise chaque mois une réunion de la CIBDU afin de débattre des dossiers sensibles ou qui appellent un examen plus approfondi. Près de 3 200 demandes de licences individuelles de biens à double usage ont été examinées en 2025. Par ailleurs, le SGDSN participe activement aux travaux européens relatifs à la mise en œuvre du règlement européen 2021/821, ainsi qu'à l'élaboration, la mise à jour et l'application des sanctions visant la Russie et la Biélorussie. La poursuite de la dégradation du contexte international renforce le besoin d'un contrôle rigoureux des exportations de ces biens et technologies sensibles.

LES RÉGIMES MULTILATÉRAUX DE CONTRÔLE DES EXPORTATIONS

Le SGDSN coordonne la définition de la position interministérielle technique française dans les quatre régimes de contrôles multilatéraux visant à prévenir la dissémination incontrôlée d'équipements et de technologies sensibles : le régime de contrôle de la technologie des missiles (MCTR), l'arrangement de Wassenaar (armement conventionnel et biens à double usage), le groupe des fournisseurs nucléaires (NSG) et le groupe Australie (armes chimiques et biologiques).

Dans ces enceintes, les États parties s'accordent sur des listes de biens à contrôler - qui sont ensuite, pour les États membres de l'UE, intégrés dans la réglementation européenne - et des lignes de conduite.

Ces régimes, qui comprennent des pays non membres de l'UE ou de l'OTAN, font actuellement face à de nombreux défis de politisation des échanges et d'instrumentalisation dans le contexte de durcissement de la compétition géostratégique.

Ils restent néanmoins des piliers irremplaçables de l'architecture internationale de sécurité et leur contribution majeure à la lutte contre la prolifération s'est poursuivie en 2025 : le travail technique a ainsi permis d'aboutir à l'adoption de nouvelles propositions d'inscriptions aux listes de contrôle (25 à Wassenaar, 1 au groupe des fournisseurs nucléaires, 4 au groupe Australie), dont plusieurs à l'initiative de la France. Aucune proposition technique n'a été adoptée par le MTCR.

— LA PROTECTION DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION (PPST)

Les risques de prédation de certains savoirs et savoir-faire sensibles, de dissémination non contrôlée au profit de capacités militaires adverses ou de détournement à des fins proliférantes et terroristes se sont significativement accrus ces dernières années. Ces risques émanent de compétiteurs stratégiques de plus en plus affirmés sur la scène internationale, et ce alors que l'architecture de sécurité internationale se fragilise.

Déployé depuis 2012, le dispositif de protection du potentiel scientifique et technique de la nation (PPST) a fait la preuve de sa pertinence et son utilité. Une mise à jour réglementaire du dispositif a eu lieu en 2024 et visait à clarifier les textes, simplifier le dispositif et renforcer sa portée, notamment par l'instauration d'un volet contraventionnel. Après la publication d'un décret en mai 2024 puis d'un arrêté en octobre 2024, la réforme du dispositif a été parachevée avec la publication le 28 avril 2025 d'une instruction interministérielle. Les premiers résultats de ces travaux réglementaires ont d'ores et déjà été observés. En outre, des travaux ont été engagés sur la prévention des débauchages de chercheurs et se poursuivront au cours de l'année 2026, dans une dynamique de renforcement global de la protection de la recherche.

EXERCICE PSI À TOULON AU PRINTEMPS 2025

Lancée en 2003, l'initiative de sécurité contre la prolifération (*Proliferation Security Initiative,* PSI) est un cadre de coopération multilatéral, volontaire et flexible visant à lutter contre le trafic d'armes de destruction massive, leurs vecteurs et les technologies connexes. Les 116 pays qui ont rejoint la PSI ont endossé les principes dits « de Paris » qui les invitent à adopter des mesures nationales pour interdire les transferts de flux proliférants et intercepter les cargaisons de marchandises suspectes.

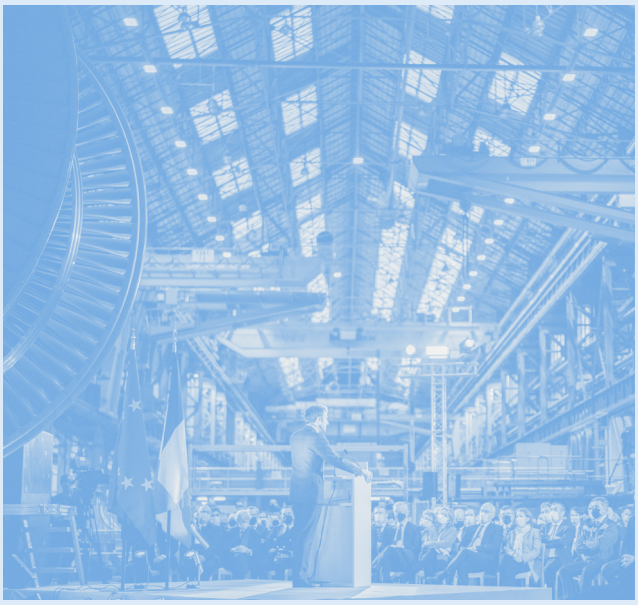
La PSI est déclinée dans le cadre de différents formats régionaux, permettant d'entretenir un dialogue entre les différents États actifs d'une même aire géographique confrontés à la prolifération. L'initiative Méditerranée, créée en 2013 par la France et l'Allemagne, rejoints par l'Italie en 2023, a ainsi vocation à renforcer la coopération régionale, dans la lutte contre la prolifération face aux enjeux de prolifération propres au bassin méditerranéen.

Le SGDSN, le ministère des armées et le ministère de l'Europe et des affaires étrangères ont organisé une nouvelle édition de l'initiative Méditerranée baptisée « Golden Isles », qui s'est tenue à Toulon les 28 et 29 avril 2025. Ce séminaire, qui a réuni 14 pays, a été l'occasion d'étudier des cas concrets et d'aborder les moyens de surmonter les difficultés rencontrées dans le cadre de la mise en œuvre d'opérations d'interception de matériels susceptibles de contribuer à des programmes d'armes de destruction massive. La France a démontré et partagé son savoir-faire opérationnel grâce à un exercice réel grandeur nature (LIVEX) simulant l'interception d'un navire suspecté de transporter une cargaison proliférante sur le porte-hélicoptère amphibie (PHA) Tonnerre, avec une intervention de la Marine nationale, du 2e régiment de dragons de l'armée de Terre, dont la spécialité est de traiter les menaces nucléaires, radiologiques, biologiques et chimiques (NBRC), ainsi que d'une équipe des douanes.

Cet événement succède à l'édition de l'initiative Méditerranée qui s'était tenue à Paris en juin 2022 ainsi qu'à plusieurs autres activités de la PSI conduites dans le cadre de ses déclinaisons régionales.

— ACCOMPAGNEMENT DE LA RELANCE DU NUCLÉAIRE

Le discours du Président de la République, prononcé à Belfort le 10 février 2022, a marqué la relance du nucléaire civil français, dont la mesure la plus symbolique est un programme ambitieux de construction de six réacteurs EPR2 de dernière génération, avec une option pour huit réacteurs supplémentaires. La gouvernance du programme nucléaire national est confiée depuis 2008 au conseil de politique nucléaire (CPN), instance présidée par le Président de la République. Le SGDSN assure le secrétariat du CPN. A ce titre, le secrétaire général, appuyé par le Haut-commissaire à l'énergie atomique (HCEA) qui lui est rattaché, assure la préparation des délibérations et le suivi de la mise en œuvre des actions. Le CPN s'est réuni en moyenne une fois par an depuis 2022 et a défini les grandes orientations de la filière nucléaire française, en particulier en matière de construction de réacteurs et de cycle du combustible. Il a également confirmé une ambitieuse stratégie de soutien aux projets de petits réacteurs *small modular reactor/advanced modular reactor* dits SMR/AMR à travers le plan d'investissement France 2030.



— SÉCURITÉ SPATIALE ET PARTICIPATION AUX TRAVAUX SUR L'EUROPE DE L'ESPACE

Dans le domaine spatial caractérisé par un duopole américano-chinois croissant, l'Europe doit relever le défi de l'autonomie et de la souveraineté. Les enjeux de sécurité et de résilience des infrastructures spatiales sont aujourd'hui d'autant plus critiques que nos économies et modes de vie en sont tributaires.

En 2025, le bureau des affaires spatiales (BAS) a été fortement impliqué dans la montée en puissance des enjeux spatiaux dans le cadre européen : mise en œuvre du contrat de concession d'IRIS², autorisation en décembre 2025 d'opérer les premiers services Govsatcom, poursuite de l'opérationnalisation des services proposés par le programme de radionavigation et de positionnement Galileo, ou encore projet pilote de service gouvernemental d'observation de la Terre EOGS. Ces travaux nécessitent une forte coordination avec les différents ministères concernés, l'UE et les représentants d'autres États membres. Le SGDSN assure ainsi la coordination interministérielle sur l'ensemble des enjeux de sécurité des différentes composantes du programme spatial européen (Galileo, Egnos, Copernicus, *Space Situationnal Awareness* et Govsatcom/IRIS²).

En outre, le SGDSN est mobilisé par les négociations en cours du *EU Spact Act* et du Fonds Européen de Compétitivité. Le SGDSN suit également avec vigilance les premières discussions sur un projet de règlement attendu au premier trimestre 2026 qui fixera le rôle de l'Agence spatiale pour le programme spatial de l'UE (EUSPA). Sa gouvernance opérationnelle devra permettre d'assurer la continuité et la résilience des services spatiaux de l'UE, y compris en temps de crise ou de guerre.

En tant qu'autorité nationale responsable de la sécurité du signal protégé *public regulated service - PRS* offert par le système de radionavigation Galileo, le SGDSN a poursuivi l'instruction des demandes d'autorisation des industriels français à travailler sur le module de sécurité et le récepteur associés à ce signal. Ce travail donne lieu, depuis 2024, à des audits périodiques des sites concernés. Cette fonction d'autorité nationale compétente est également exercée depuis 2023 dans le cadre du programme de communications satellitaires européen (Govsatcom) et de la future constellation sécurisée IRIS[2], pour lesquels les travaux d'identification des potentiels utilisateurs et de leurs usages se sont poursuivis.

Le SGDSN a, en coopération avec le ministère de l'Europe et des affaires étrangères, continué de s'impliquer dans les dialogues spatiaux afin d'entretenir un cadre d'échange sur les enjeux stratégiques. Ces cadres d'échange permettent aussi d'assurer le suivi des programmes de coopération engagés par nos agences spatiales respectives.

Enfin, le bureau des affaires spatiales a largement contribué à l'élaboration de la stratégie nationale spatiale, et en particulier aux travaux approfondis dans le domaine des lanceurs, des technologies critiques et de la coopération internationale spatiale. Les travaux de mise en œuvre de cette stratégie ont débuté, et font l'objet d'un suivi interministériel attentif.

TRAVAUX SUR LES TECHNOLOGIES CRITIQUES DU SPATIAL

Dans le cadre de l'élaboration de la stratégie nationale spatiale[2], le SGDSN a été chargé de coordonner les travaux interministériels d'identification des technologies critiques à horizon 2040, avec le double objectif :

- d'établir la liste des technologies à développer de manière souveraine,
- d'identifier les champs de coopération européenne et internationale dans ce domaine.

Menés avec l'appui du CNES et des ministères de l'économie, de la recherche et des armées, ces travaux ont permis de recenser quelques technologies de rupture - certaines encore peu matures - susceptibles de bouleverser les équilibres spatiaux.

Ils devront permettre de prioriser plus efficacement les efforts financiers de l'État et de mieux cerner les technologies devant faire l'objet de coopérations européennes ou internationales.

Le rythme rapide des évolutions technologiques dans le domaine spatial impose une revisite régulière, qui se poursuivra au cours des prochaines années, en coordination avec les travaux similaires menés à l'échelle européenne.

— ANTICIPATION STRATÉGIQUE

Le SGDSN est chargé d'animer, au niveau interministériel, la fonction d'anticipation stratégique dans le domaine de la défense et de la sécurité nationale. À ce titre, il pilote le comité interministériel d'anticipation qui, depuis 2021, réunit deux fois par an une dizaine de ministères, la CNRLT et le Haut-commissariat à la stratégie et au plan. Ces travaux s'attacheront de plus en plus à l'identification des technologies les plus disruptives et leurs effets sur la sécurité nationale afin de permettre l'identification des scénarios de rupture et de mieux y préparer le pays.

[2] Disponible sur le site du SGDSN : https://www.sgdsn.gouv.fr/publications/strategie-nationale-spatiale-2025-2040

AGNÈS ROMATET-ESPAGNE

Directrice des Affaires Internationales,
Stratégiques et Technologiques

« Ce scénario central fixe le niveau de l'effort général de préparation que la RNS considère comme pertinent »

L'année 2025 a été marquée par les travaux d'actualisation de la Revue nationale stratégique. Dans quelle mesure se travail va-t-il se prolonger cette année pour votre direction ?

L'actualisation de la Revue nationale stratégique (RNS), présentée par le Président de la République le 13 juillet dernier, prend acte de la remise en cause des fondements du système international tel que nous le connaissions. Elle en tire les conséquences en formulant le scénario central de la survenance, dans les prochaines années, d'un conflit de haute intensité en Europe ou aux frontières de l'Europe, accompagné d'attaques hybrides massives sur notre territoire. Ce scénario central fixe le niveau de l'effort général de préparation que la RNS considère comme pertinent.

Pour y parvenir, la RNS fixe une feuille de route pour l'ensemble des ministères et, au-delà, pour l'ensemble de la Nation. La direction des affaires internationales, stratégiques et technologiques sera particulièrement mobilisée par la mise en œuvre de trois objectifs stratégiques.

Le premier concerne la préparation de l'économie nationale à la guerre, ce qui suppose de protéger la base industrielle et technologique de défense mais surtout de soutenir son développement à l'exportation, dans le respect de nos engagements internationaux.

Le deuxième traite des menaces hybrides auxquelles notre pays pourrait être confronté, tout particulièrement dans les cinq champs prioritaires que sont le cybersepace, la sphère informationnelle, l'économie, le droit (*lawfare*) et au travers d'opérations militaires. Face à ces menaces, notre organisation interministérielle doit être capable d'identifier et de caractériser des agissements relevant du champ de l'hybridité, et d'y réagir.

Le troisième traite de la préservation de l'excellence académique, scientifique et technologique nationale. Notre action en 2026 visera notamment à s'assurer que nos savoir-faire et technologies sensibles soient mieux protégés lorsque c'est nécessaire, tant au travers du contrôle des exportations que de l'encadrement des coopérations internationales. En outre, la prévention des débauchages de nos chercheurs dans les domaines les plus critiques sera un axe de travail important pour la première partie de l'année 2026, dans le cadre de l'actualisation de la loi de programmation militaire.

Que vous inspire la stratégie de sécurité économique publiée par la Commission européenne à la fin de l'année 2025 ?

Dans sa doctrine, la Commission européenne fait preuve d'un volontarisme notable et évoque de nombreuses pistes de travail, dont certaines doivent être approfondies. Le SGDSN s'impliquera dans les travaux européens à venir, au travers des canaux habituels du SGAE et de notre représentation permanente. Certains sujets feront l'objet d'une vigilance particulière : instauration d'une préférence européenne, évaluation du règlement relatif à l'exportation de BDU (*cf. infra*), mise en place d'un outil de contrôle des investissements entrants et sortants, travaux sur la sécurité de la recherche. Enfin, de manière plus concrète, ces réflexions conduiront à des échanges et des partages d'information dont la sécurité devra être garantie. ▸▸▸

Nous assistons à un net raidissement du contrôle des exportations dans le monde, comment votre direction aborde-t-elle ses missions dans ce domaine ?

Nous constatons en effet une extension des listes de biens contrôlés, un renforcement des formalités et des procédures de vérification, mais également une volonté de certains États d'instrumentaliser ces dispositifs à des fins de sécurité économique.

Le contrôle des exportations de biens sensibles – je pense aux matériels de guerre et aux biens à double usage – participe de la lutte contre la prolifération d'armes conventionnelles et de destruction massive, ainsi que de leurs vecteurs et du respect des engagements internationaux de la France. Il constitue, à cet égard, l'une des missions principales de la direction au travers de la présidence de la CIEEMG et de la CIBDU. Nous poursuivrons en 2026 ce travail avec la rigueur et l'exigence dont nous avons toujours fait preuve.

Parallèlement, le SGDSN maintiendra sa participation active aux dialogues multilatéraux, aux régimes de contrôles en matière de contrôle des exportations et aux discussions en cours au niveau européen. Il s'y assurera de la préservation des prérogatives relevant de la sécurité nationale et du bon respect de la distinction entre sécurité économique et sécurité nationale. À défaut, la confusion entre ces notions pourrait être de nature à fragiliser et fragmenter l'architecture de sécurité internationale. ◂

3

RENFORCER LE NIVEAU DE PRÉPARATION

RESISTER

— UNE CYBERMENACE PLUS COMPLEXE À APPRÉHENDER

En 2025, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) constate une stabilisation du nombre d'incidents (1 366), c'est-à-dire des événements au sujet desquels l'ANSSI peut confirmer que l'action d'un acteur malveillant a produit des effets sur un système d'information. Le niveau de gravité de ces incidents demeure élevé, après une croissance importante depuis 2022.

Le principal enseignement de l'année 2025 est la complexité grandissante des cybermenaces qui ciblent les intérêts français. Ce phénomène s'explique notamment par la disparition progressive des frontières entre acteurs étatiques et cybercriminels, qui utilisent les mêmes outils et techniques d'attaque et emploient de surcroît des techniques de dissimulation de traces qui contribuent à brouiller les pistes.

Les principaux acteurs de la menace demeurent des modes opératoires réputés russes et chinois et, dans un contexte de tensions géopolitiques croissantes, l'ANSSI constate en 2025 un effort continu de ciblage des intérêts diplomatiques français à des fins de collecte de renseignement stratégique. Ces acteurs attaquent aussi des infrastructures importantes au fonctionnement des réseaux de télécommunication ou de distribution d'énergie – en France et plus largement en Europe – et parviennent régulièrement à en affecter le fonctionnement.

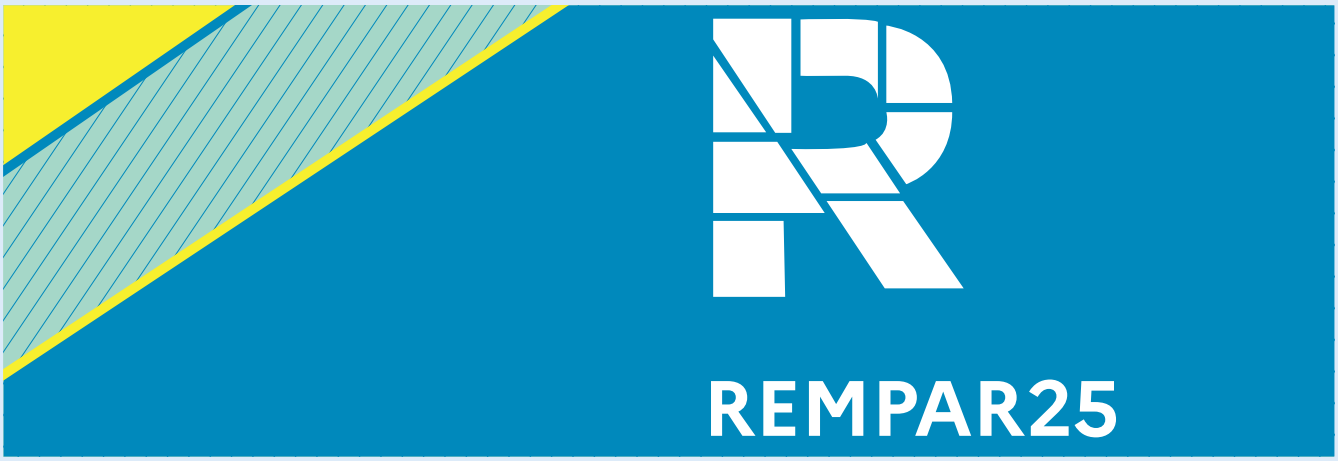
— REMPAR25 : UN EXERCICE DE CRISE CYBERSÉCURITAIRE D'UNE AMPLEUR INÉDITE

La Revue nationale stratégique actualisée parue le 14 juillet 2025 et la Stratégie nationale de cybersécurité publiée au mois de janvier 2026 font de la cyber-résilience du pays un objectif stratégique à part entière. L'exercice de crise d'origine cybersécuritaire REMPAR25, organisé au mois de septembre, s'est inscrit concrètement dans cet objectif en permettant une montée en compétences rapide et massive de 1 263 organisations publiques et privées.

Plus de 5 600 professionnels ont ainsi participé à cet exercice, organisé par l'ANSSI en partenariat avec le Club de la continuité d'activité, le Club de la sécurité de l'information français, le Club des experts de la sécurité de l'information et du numérique et le Campus Cyber national, dans 13 régions et 7 territoires d'outre-mer.

REMPAR25 a consisté à simuler une crise cybersécuritaire systémique, entraînant une interruption massive des services numériques essentiels. Pour la première fois, entreprises, administrations et acteurs territoriaux ont pu s'immerger dans une crise majeure de cette nature, révélant l'importance cruciale des plans de continuité d'activité. De plus, l'un des enjeux de l'exercice résidait dans la coordination entre les différents niveaux de réponse, local et national. Plus de 50 partenaires, dont les Campus Cyber régionaux, des centres de réponse à incident cyber *(CSIRT* pour *Computer Security Incident Response Team)* territoriaux et sectoriels, des associations professionnelles et des services de l'État, ont ainsi contribué à l'organisation de l'exercice.

Pour 95 % des participants, quels que soient leur taille ou leur secteur d'activité, REMPAR25 a été l'occasion de mettre en œuvre des actions en matière de gestion de crise et de sécurité des systèmes d'information.



— CONTRIBUTION AU DÉVELOPPEMENT D'UNE IA DE CONFIANCE

En tant qu'autorité nationale de cyberdéfense et de cybersécurité, l'ANSSI travaille à l'identification et la bonne compréhension des risques cybersécuritaires des systèmes d'intelligence artificielle, en collaboration avec ses partenaires nationaux et internationaux. Afin d'accompagner le développement d'une intelligence artificielle de confiance qui bénéficie à tous et pour tous les usages, quelle que soit leur sensibilité, l'Agence promeut une approche par l'identification, l'évaluation et la gestion des risques.

Pour guider les dirigeants et les producteurs de solutions d'IA, l'ANSSI a notamment porté deux actions lors du sommet pour l'action sur l'intelligence artificielle, organisé à Paris en février 2025.

Elle a publié un document de référence *Développer la confiance dans l'IA par une approche par les risques cyber*, co-signé par 19 partenaires internationaux et 5 partenaires nationaux, qui met en évidence les risques de cybersécurité auxquels sont exposés les systèmes d'intelligence artificielle et promeut les principales recommandations stratégiques afin de favoriser une meilleure prise en compte de la cybersécurité dans le développement et l'intégration de ces systèmes. Elle a également organisé un exercice de gestion de crise cyber, le 11 février, au Campus Cyber, qui a mobilisé près de 200 participants nationaux et internationaux, experts en cyber et en intelligence artificielle, dans l'objectif de développer une meilleure compréhension mutuelle de leurs enjeux.

STRATÉGIE DE RÉPONSE RELATIVE À APT28

Le 29 avril 2025, par la voix du ministre de l'Europe et des affaires étrangères, la France condamnait le recours par le service de renseignement militaire russe (GRU) au mode opératoire d'attaque (MOA) APT28 pour mener plusieurs cyber-attaques contre des intérêts français.

Cette première attribution publique française est issue d'un travail conjoint du Centre de coordination des crises cyber (C4), composé de l'ANSSI, de la Direction générale de la sécurité intérieure (DGSI), de la Direction générale de la sécurité extérieure (DGSE), du Commandement de cyberdéfense (COMCYBER), de la Direction générale de l'Armement (DGA) et des services du ministère de l'Europe et des affaires étrangères (MEAE). Sous l'égide du SGDSN, le C4 permet un échange d'analyses relatives aux cybermenaces et propose des stratégies de réponse globales de l'État aux agressions cyber, sur la base de leviers de réponse variés.

Ici, les analyses du C4 ont permis d'attribuer formellement au GRU, employant le MOA APT28, le ciblage ou la compromission d'une dizaine d'entités françaises depuis 2021 : services publics, entreprises privées, entité sportive liée à l'organisation des jeux Olympiques et Paralympiques de 2024. Avant cette date, le C4 peut confirmer que APT28 a également été utilisé par le GRU dans le sabotage de la chaîne de télévision TV5 Monde en 2015, ainsi que dans la tentative de déstabilisation du processus électoral français en 2017. Enfin, APT28 est aussi employé pour exercer une pression constante sur les infrastructures ukrainiennes dans le contexte de la guerre d'agression menée par la Russie contre l'Ukraine, notamment lorsqu'il est opéré par l'unité 20728 du GRU.

Cette dénonciation publique inédite illustre que la France s'est donnée les moyens – au travers du C4 – de détecter, contrer et dénoncer ces opérations, et ce dans un contexte d'aggravation des tensions géopolitiques mondiales.

— CHIFFRES CLÉS DE L'ANSSI EN 2025

1 366 incidents

16 logiciels publiés en *open source*

22 articles scientifiques publiés

369 qualifications

1 543 personnes formées

130 certifications

3 586 événements de sécurité

499 visas de sécurité délivrés

1 avis technique publié

147 027 attestations SecNumAcadémie délivrées

17 formations labellisées SecNumEduc-FC

26 formations labellisées SecNumEdu

28 guides techniques publiés

VINCENT **STRUBEL**

Directeur de l'Agence nationale
de la sécurité des systèmes d'information

« Nous avons pu avancer sur des chantiers importants en lien avec les technologies dites de rupture »

Que retenez-vous de l'année 2025 et quels ont été les jalons marquants pour l'ANSSI ?

L'année 2025 a été particulièrement structurante pour l'ANSSI. Nous avons pu avancer sur des chantiers importants en lien avec les technologies dites de rupture, telles l'intelligence artificielle et la cryptographie post-quantique. Le sommet pour l'action sur l'IA a été à ce titre un temps marquant. Ayant particulièrement mobilisé les équipes de l'ANSSI, il a permis d'aboutir à la signature, par 19 partenaires internationaux et 5 partenaires nationaux, d'une déclaration pour assurer le développement d'une IA de confiance grâce à une approche fondée sur l'identification, l'évaluation et la gestion des risques cybersécuritaires. Cette déclaration a permis de nourrir les travaux internes sur la sécurisation de l'intelligence artificielle qui vont continuer de nous occuper pour les prochaines années. Sur la cryptographie post-quantique, des actions essentielles ont également été conduites en 2025, avec notamment la mise à disposition de recommandations et d'informations utiles pour la préparation des organisations à cette transition.

En parallèle, nous avons avancé sur l'application des nouvelles réglementations particulièrement attendues pour élever le niveau général de cybersécurité. Sur la mise en œuvre du Règlement européen sur la résilience cyber *Cyber Resilience Act* - CRA, dont les premières applications commenceront à partir de juin 2026, et qui imposera notamment aux fournisseurs de produits numériques de notifier leurs vulnérabilités et d'appliquer un certain nombre d'exigences de cybersécurité, l'organisation nationale a été définie. La mise en œuvre de cette réglementation se fera en étroite collaboration avec l'Agence nationale des fréquences (ANFR), en qualité d'autorité de surveillance de marché à même de sanctionner ceux qui ne respecteraient pas les règles du jeu. L'année 2025 nous a encore démontré que l'absence de mesures de cybersécurité sur certains produits numériques et une gestion déficiente des vulnérabilités avaient conduit à de trop nombreuses cyberattaques.

À côté du CRA, nous avons continué à travailler sur la préparation de la mise en œuvre de la directive sur la sécurité des réseaux et des systèmes d'information, dite *NIS2*, dont la transposition par le projet de loi Résilience devrait aboutir prochainement. Elle permettra d'améliorer le niveau de cybersécurité de plus de 20 000 entités en France. Le travail de co-construction avec les différentes parties prenantes s'est poursuivi, en particulier sur le référentiel de mesures de cybersécurité qui pourra être utilisé par les entités régulées dans leur travail de sécurisation et de mise en conformité. Ce travail continuera en 2026 afin d'accompagner les entités à élever leur niveau de cybersécurité.

Face à une menace prégnante, quelle est la réponse de l'ANSSI ?

Les attaquants n'attendent pas que nous mettions en œuvre le nouveau cadre réglementaire pour attaquer nos entreprises, collectivités ou administrations, et l'adversité a encore été forte en 2025.

Face à ce constat, les équipes de l'ANSSI travaillent à sensibiliser, préparer et à prévenir les futures attaques. C'est un effort quotidien et permanent qui permettra d'assurer cette élévation générale du niveau de cybersécurité. Nous y contribuons notamment grâce à des exercices de gestion de crise à grande échelle, à l'image de REMPAR25. Ces exercices permettent de réunir les différents acteurs de l'écosystème cyber au ▸▸▸

niveau national, européen et dans les territoires, et d'accompagner les entités à gagner en maturité sur la gestion d'une crise. Ils permettent également de structurer et renforcer notre dispositif national de cybersécurité. À ce titre, l'ANSSI a ouvert en 2025 un appel à manifestation d'intérêt pour le renforcement de l'accompagnement local aux enjeux de cybersécurité. La démultiplication des capacités d'assistance et d'accompagnement de proximité qu'apportent notamment les *CSIRT* territoriaux est primordiale pour mieux prendre en compte la totalité des acteurs économiques et sociaux, et faire face à la menace.

Enfin, pour assurer une meilleure résilience de la Nation, il est nécessaire de faire évoluer notre gouvernance nationale de cybersécurité ; ce que prévoit la Stratégie nationale de cybersécurité 2026-2030. L'objectif est de développer et mieux coordonner les politiques publiques concourant au renforcement de la cybersécurité de tous les pans de la société. Plus globalement, l'objectif est de mieux intégrer les parties prenantes, et en particulier les territoires, dans cette gouvernance.

Quelles sont les perspectives de l'ANSSI pour 2026 ?

Tout d'abord, la poursuite de la préparation de la mise en œuvre de la directive *NIS* 2. Les entreprises, administrations et collectivités seront sur ce point accompagnées durant toute l'année par la mise à disposition de différents outils. Il est essentiel pour les entités d'enclencher dès à présent, notamment pour les moins matures d'entre elles, l'anticipation de ces mesures. La préparation des premiers contrôles que l'ANSSI mènera sur les entités sera également un volet important de l'année 2026. Elle sera précédée d'un travail de définition de la stratégie de contrôle voulue par l'Agence.

Nous inaugurerons par ailleurs le nouveau cadre fixé par le CRA. Les fournisseurs de produits numériques devront notifier à l'ANSSI les vulnérabilités affectant leurs produits. En parallèle, la structuration de l'organisation avec l'ANFR sera essentielle dans la perspective des premiers contrôles que pourra conduire cette dernière. Un important travail de normalisation au niveau européen sera également suivi par les équipes de l'ANSSI pour assurer l'établissement des normes spécifiques et horizontales qu'imposera le CRA aux fournisseurs de produits numériques. D'autres négociations, particulièrement importantes pour l'Agence, seront également suivies au niveau européen en 2026 avec en premier lieu la révision du Règlement sur la cybersécurité *Cybersecurity Act* - CSA comprenant des volets importants pour l'ANSSI relatifs à la certification des produits et services numériques, au mandat de l'Agence européenne de cybersécurité (ENISA) ou encore à la prise en compte de certains risques liés à des technologies particulièrement critiques. D'autres textes seront également suivis par l'Agence, notamment l'Omnibus numérique visant à simplifier et à clarifier l'articulation de précédents textes européens.

Enfin, la sécurisation des nouveaux grands événements nous occupera également en 2026 et 2027, avec en premier lieu la sécurisation des élections municipales, puis la préparation du G7 et enfin des élections présidentielle et probablement législatives de 2027. Dans une perspective plus lointaine mais néanmoins nécessaire à entamer dès à présent, la sécurisation des jeux Olympiques et Paralympiques (JOP) d'hiver de 2030 continuera également d'être suivie cette année, en capitalisant sur notre retour d'expérience des JOP 2024. ◂

4

PARTICIPER À LA CONTINUITÉ DE L'ÉTAT

ENGAGER

En 2025, l'OSIIC a fêté ses cinq années d'existence dans un contexte de tensions internationales et d'évolutions des menaces qui l'ont amené à adapter sa stratégie pour soutenir la décision et l'action gouvernementales et interministérielle.

Durant cette année, placée sous le double signe de la sécurité informatique et du service aux utilisateurs, l'opérateur a franchi les jalons de la trajectoire devant l'amener à renforcer la résilience interministérielle garante de la continuité de l'État conformément à sa feuille de route stratégique 2024-2027[3].

— UN SERVICE RENDU AVEC ENGAGEMENT ET RÉACTIVITÉ

Parmi les missions essentielles de l'OSIIC figure l'accompagnement des très hautes autorités de l'État dans leurs déplacements. En 2025, l'opérateur a assuré les communications sécurisées lors de 34 voyages officiels.


© Présidence de la République

Il a aussi poursuivi la modernisation des liaisons internationales du Président de la République afin de garantir la disponibilité et la confidentialité de ces moyens. L'extension de ce dispositif vers de nouveaux interlocuteurs permet désormais de communiquer avec l'ensemble des autorités de l'Union Européenne au travers du système mis en place par le Secrétariat Général du Conseil de l'Union Européenne.

Dans le champ de l'interministérialité, le déploiement des moyens de communication classifiés s'est fait conformément aux orientations de la programmation annuelle. 35 nouveaux sites sont désormais équipés et 280 terminaux interministériels classifiés supplémentaires ont été déployés. La conclusion d'une convention avec le ministère de l'Europe et des affaires étrangères (MEAE) offre un cadre au partenariat stratégique avec l'OSIIC. Celui-ci permet de généraliser le déploiement des systèmes de l'opérateur dans les postes diplomatiques à l'étranger et d'en permettre l'accès à l'ensemble des fonctionnaires – tous ministères confondus – présents au sein de l'ambassade.

© Présidence de la République

Par ailleurs, des travaux ont également été conduits afin de faire évoluer significativement le système d'exploitation Secdroid utilisé par l'ensemble des agents du SGDSN, ainsi que 230 000 gendarmes et policiers *via* la déclinaison NEO2 en service au sein du ministère de l'intérieur. Cette nouvelle version a été réalisée en partenariat avec l'agence nationale des forces de sécurité intérieure (ANFSI). Au-delà, les travaux préparatoires au futur marché relatif au système qui succédera à NEO2 ont débuté entre l'ANFSI et l'OSIIC, avec le soutien de l'agence nationale de la sécurité des systèmes d'information (ANSSI).


© Présidence de la République

NEO2

S'appuyant sur le système d'exploitation sécurisé Secdroid dérivé d'Android, développé et maintenu par l'OSIIC en partenariat avec l'ANSSI, le terminal mobile NEO2 est un produit de l'agence nationale des forces de sécurité intérieure (ANFSI) au profit des forces de sécurité intérieure. Il équipe 265 000 agents dans leurs missions quotidiennes, particulièrement en matière de sécurité publique. Utilisé en conjonction avec Secdroid, le terminal fourni par la société française Crosscall, acquis *via* le marché NEO2, offre un environnement de travail hautement sécurisé.

[3] Disponible sur le site du SGDSN : https://www.sgdsn.gouv.fr/publications/osiic-une-nouvelle-feuille-de-route-strategique-qui-fixe-le-cap

— UNE TRANSFORMATION NUMÉRIQUE AU SERVICE DES UTILISATEURS DU SGDSN

Tout en maintenant un haut niveau de satisfaction de ses utilisateurs, l'OSIIC relève les défis de modernisation et d'extension de ses services. Le baromètre semestriel de satisfaction montre ainsi une nette progression entre 2023 et 2025 avec un accroissement de 2,5 points de la satisfaction moyenne au dernier semestre et une progression du *Net Promoter Score*[4] de 57 points sur les deux dernières années. Les utilisateurs saluent notamment la qualité de service, le développement de nouveaux produits et la meilleure stabilité des systèmes.

Au cœur des attentes de nos bénéficiaires, la modernisation de nos outils numériques est passée par de nouvelles versions majeures des terminaux et des applicatifs pour mettre à disposition les fonctionnalités les plus avancées, tout en continuant de prendre en compte les impératifs de sécurité. Par ailleurs, cette modernisation est naturellement passée par la poursuite de la transformation numérique des usages, comme le parapheur électronique pour tous les niveaux de sensibilité d'information et le développement de nouveaux outils permettant l'utilisation de données classifiées. Le recours à l'intelligence artificielle a fait l'objet d'expérimentations et une feuille de route a été initiée, prenant en compte un possible partenariat avec le ministère des armées.

L'opérateur a poursuivi les travaux de fiabilisation du réseau de travail interne du SGDSN engagés depuis 2023. Ils ont notamment porté sur la mise à jour, des chaînes d'authentification ainsi que de la chaîne de navigation utilisée sur internet. Il s'agit là d'un renforcement significatif de la sécurité des systèmes d'information. De surcroît, les utilisateurs en retireront des bénéfices tangibles, grâce à l'amélioration de la qualité des visioconférences réalisées depuis les postes de travail.

De même, les travaux d'expérimentation d'un nouveau réseau de stations-blanches a abouti à des conclusions positives. Ces stations sont en cours d'installation sur les différents sites du SGDSN depuis le début de l'année 2026. Elles permettront aux agents du SGDSN de disposer d'une solution facile d'emploi et techniquement robuste de contrôle et de nettoyage des clés USB à usage professionnel.

Enfin, la résorption de la dette technique s'est poursuivie. Elle a pris diverses formes dont la migration des utilisateurs de l'ancien réseau Secret du SGDSN vers ISIS, le décommissionnement des serveurs, systèmes et moyens de communication devenus obsolètes, et l'extinction du système de phonie SOLANGE qui a assuré les communications classifiées du Président de la République pendant de nombreuses années.

CHIFFRES CLÉS 2025

265 000 téléphones mobiles déployés auprès des forces de sécurité intérieure

9 000 utilisateurs des systèmes interministériels classifiés

+ 700 sites équipés en systèmes d'information interministériels classifiés dans l'hexagone, en outre-mer et dans 100 ambassades françaises

365 jours d'assistance SECRET joignable 24h/24

37 M€ de budget annuel

1 400 utilisateurs au sein du SGDSN

8 *hubs* interministériels

100 % de couverture des besoins de réseaux classifiés de la sphère civile de l'État, hors services de renseignement

[4] Le *Net promoter score* (NPS) est un outil de gestion largement reconnu et utilisé pour mesurer la satisfaction des clients. Il mesure le pourcentage de clients très satisfaits (*promoteurs*) pondéré par le pourcentage de clients insatisfaits (*détracteurs*).

YVES **VERHOEVEN**

Directeur de l'Opérateur des Systèmes d'Information Interministériels Classifiés

« La disponibilité de réseaux de très haute sécurité est essentielle pour la gestion des affaires de l'État »

Quelles sont les événements marquants de l'année 2025 pour l'OSIIC ?

Malgré une actualité politique et un contexte budgétaire particuliers durant l'année écoulée, l'OSIIC et ses agents ont su s'adapter et faire preuve de professionnalisme pour remplir leurs missions en toutes circonstances, en mettant systématiquement la sécurité et le service aux utilisateurs au centre de leur action. Le maintien d'un haut niveau de satisfaction des bénéficiaires des services de l'opérateur, alors que nous avons dans le même temps procédé à des opérations techniques lourdes et accaparantes, comme les mises à jour techniques majeures, la migration d'infrastructures de gestion de clés et l'actualisation des systèmes d'exploitation et des logiciels bureautiques, atteste de notre capacité à remplir nos missions en toutes circonstances.

Je considère notre capacité à mener à bien diverses opérations lourdes simultanément comme la marque d'une forme de maturité, alors même que 2025 marque le 5e anniversaire de l'OSIIC. Cette maturité est probablement l'alliage d'une capacité à faire plus, à faire mieux et à rester fidèle à notre vocation initiale résolument interministérielle. Ce caractère interministériel est conforté par l'attribution à l'opérateur de la conduite d'un nouveau programme interministériel classifié très attendu par ses futurs clients.

Quels sont les défis à venir pour l'opérateur ?

Nous avons collectivement fait le constat que si nous parvenons actuellement à réaliser nos missions, nos méthodes ne sont pas à jour. Nous nous épuisons régulièrement dans une action transversale qui manque de fluidité, alors même que l'adoption de méthodes plus modernes permettrait de réduire les frictions internes. Il en résulterait aussi bien un gain de performance que de qualité de vie pour nos agents.

Parallèlement, les nouveaux projets ambitieux qui nous sont confiés nous amènent à recruter. Si l'OSIIC se montre attractif par ses missions porteuses de sens au quotidien, les nouveaux talents que nous intégrons se montrent légitimement exigeants sur l'adoption par l'OSIIC des méthodes les plus modernes.

Pour ces raisons, nous avons ressenti le besoin de faire évoluer nos pratiques. Le lancement d'une mission d'accompagnement par la direction interministérielle de la transformation publique (DITP) et la multiplication des discussions avec les agents nous ont permis d'engager un travail de transformation de l'opérateur lors du dernier trimestre de l'année 2025. Les conclusions de ces travaux sont attendues au début du deuxième trimestre 2026 pour permettre leur mise en œuvre dans la foulée. C'est un enjeu majeur pour l'opérateur ! ▸▸▸

Comment l'OSIIC anticipe-t-il l'évolution des menaces et les enjeux de souveraineté ?

Dans un contexte de tensions internationales qui nous rappelle quotidiennement l'ampleur des enjeux de souveraineté, la disponibilité de réseaux de très haute sécurité, aptes à protéger la confidentialité des informations les plus sensibles, est essentielle pour la gestion des affaires de l'État. De longue date, le développement et l'administration de réseaux protégés bénéficie du soutien des plus hautes autorités de l'État. Aujourd'hui, c'est l'OSIIC qui, pour le volet interministériel et la sphère civile de l'État, fournit les réseaux protégeant les informations classifiées au niveau Secret et en assure le bon fonctionnement en toutes circonstances. Cette mission, qui place l'opérateur au cœur du fonctionnement de l'État, nous honore et nous oblige à être lucide sur l'évolution – croissante ! – de la menace et la prise en compte au bon niveau des enjeux de souveraineté. Tout en capitalisant sur son expérience et son investissement historique dans la sécurité des systèmes d'information classifiés, l'opérateur renforce continuellement ses pratiques et ses capacités en matière de sécurité et de cybersécurité, en inscrivant ses actions dans la dynamique de la stratégie nationale de cybersécurité 2026-2030. Il ne s'agit pas pour nous de nous contenter de faire de la sécurité par la conformité, mais bien de piloter dynamiquement notre action de (cyber)sécurité par la connaissance de la menace !

Du point de vue de la souveraineté, si les lignes de défense essentielles de nos réseaux les plus sensibles reposent systématiquement sur l'emploi de briques techniques pleinement maîtrisées par la France, la volonté de défense en profondeur justifie une action permanente de renforcement de notre souveraineté. Il s'agit de rechercher en premier lieu des composants maîtrisés au niveau national, ou à défaut au niveau de l'Union européenne. Et même sur les composants les moins critiques, les approvisionnements et la sécurité de la chaîne d'approvisionnement sont devenus des problématiques incontournables. Nous sommes véritablement dans une démarche de recherche de « souveraineté en profondeur » ! ◂

5

DÉVELOPPER DE NOUVELLES CAPACITÉS

SENSIBILISER

— CHEF DE FILE NATIONAL DANS LA LUTTE CONTRE LES INGÉRENCES NUMÉRIQUES ÉTRANGÈRES (INE), VIGINUM POURSUIT L'ADAPTATION DE SES CAPACITÉS OPÉRATIONNELLES TOUT EN SE RAPPROCHANT DAVANTAGE DE LA SOCIÉTÉ CIVILE

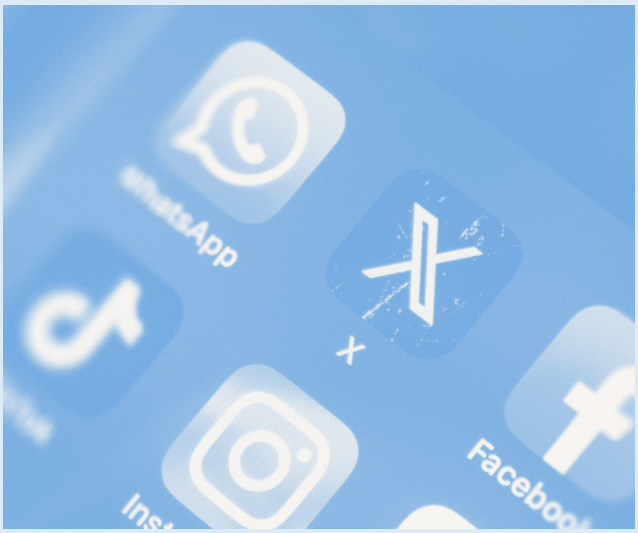
Après une année 2024 marquée par la protection du débat public numérique entourant deux scrutins électoraux et les jeux Olympiques et Paralympiques de Paris, Viginum a consacré ses efforts, en 2025, au développement de partenariats structurants et au renforcement de son modèle opérationnel.

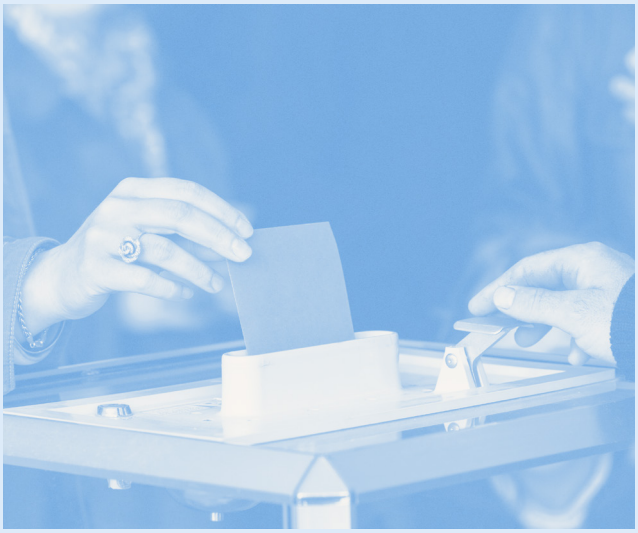
Au cours de l'année 2025, Viginum, chef de file national en matière de lutte contre les manipulations de l'information, a approfondi sa coopération avec ses partenaires interministériels. Deux feuilles de route ont ainsi été signées. L'une avec le ministère de l'Europe et des affaires étrangères, afin de structurer la promotion à l'étranger des actions de sensibilisation à la menace informationnelle ; la seconde avec le ministère de l'éducation nationale, pour élaborer de concert et intégrer dans les programmes scolaires des ressources pédagogiques. Par ailleurs, le service a poursuivi ses travaux d'accompagnement des partenaires internationaux en multipliant les actions de *capacity-building*, notamment au profit de la Moldavie ou de la Suède. Enfin, le service a contribué activement aux travaux de la Commission européenne relatifs au projet de bouclier démocratique européen.

Au cours de l'année 2025, de nouveaux partenariats avec le monde de la recherche et celui des médias ont également vu le jour. Le 28 mars, Viginum et INRIA ont ainsi signé une convention qui prévoit la création d'un laboratoire commun « IA et manipulations de l'information », ainsi que la mise en place d'un prix scientifique, destiné à stimuler et promouvoir la recherche relative aux techniques de manipulation de l'information.

Par ailleurs, Viginum et France Télévisions ont noué, à l'automne 2025, un partenariat destiné à former les journalistes aux techniques d'investigations en ligne, ainsi qu'à renforcer l'information du public sur les ingérences numériques étrangères pour accroître la résilience de notre société.

Cette exigence en matière d'information et de sensibilisation s'est notamment traduite par l'organisation, en 2025, de deux événements publics majeurs. S'inscrivant dans l'ambition portée par le Président de la République de mettre l'intelligence artificielle au service de l'intérêt général, Viginum a organisé avec l'appui de l'OCDE, à l'occasion du sommet pour l'Action sur l'IA, un événement destiné à explorer les défis et les opportunités que représente l'intelligence artificielle en matière de manipulations de l'information.





En mars 2025, Viginum a organisé son second forum académique intitulé ***Faire face ensemble pour protéger la démocratie face aux manipulations de l'information***. Rassemblant des acteurs institutionnels, internationaux et français, ainsi que des chercheurs, des représentants des médias et des ONG, cet événement a examiné les solutions dont disposent les démocraties pour faire face aux manipulations de l'information.

© VIGINUM

En outre, afin de structurer et accroître ses actions de sensibilisation, Viginum a lancé, en 2025, la préfiguration d'une académie de la lutte contre les manipulations de l'information. Cette structure, qui sera pleinement opérationnelle en 2026, aura notamment pour missions d'accompagner les acteurs institutionnels, privés, et issus de la société civile, dans leur protection face aux risques posés par les ingérences numériques étrangères (INE), et de contribuer à la résilience de la société par le développement de ressources et supports d'information.

Enfin, 2025 a été l'année du retour d'expérience et de la rénovation du cadre d'emploi de Viginum. S'appuyant sur les enseignements tirés de quatre années d'activité opérationnelle, des réflexions ont été menées avec le cabinet du secrétaire général du SGDSN, le comité éthique et scientifique ainsi que la Commission nationale de l'information et des libertés (CNIL) pour identifier les besoins d'adaptation du cadre juridique nécessaires face à l'évolution préoccupante des ingérences numériques étrangères. Partagés et consolidés, ces constats ont permis de circonscrire les ajustements du cadre réglementaire actuel souhaitables, sans remettre en cause les équilibres antérieurs qui donnent unanimement satisfaction. Parmi ces ajustements, le nouveau décret, entré en vigueur le 12 février 2026, confie de nouvelles missions au SGDSN et à Viginum en matière de lutte contre les ingérences numériques étrangères. En outre, il prévoit une évolution du cadre de collecte et de conservation des données nécessaire à l'exercice des missions de Viginum et étend notamment le champ d'action du service aux moteurs de recherche et aux outils d'intelligence artificielle conversationnelle.

— UNE ACTIVITÉ OPÉRATIONNELLE MARQUÉE PAR LA VOLATILITÉ DU CONTEXTE INTERNATIONAL ET LES MUTATIONS TECHNOLOGIQUES

L'année 2025 a été marquée par la persistance des conflits armés, la fragilisation des grands équilibres internationaux et l'apparition de nouvelles zones de tensions. Dans ce contexte géopolitique instable, l'état de la menace informationnelle s'est sensiblement dégradé. Notamment amplifiée par la numérisation croissante de nos usages et une accélération des innovations technologiques, la menace informationnelle s'est imposée comme un défi majeur affectant l'ensemble des démocraties, particulièrement en période électorale. Événement sans précédent, l'annulation du premier tour de l'élection présidentielle roumaine par la cour constitutionnelle, le 6 décembre 2024, a ainsi provoqué une prise de conscience générale de la menace que représentent les ingérences numériques étrangères, notamment lors des grands rendez-vous démocratiques.

Dans ce contexte de compétition stratégique exacerbée, Viginum observe à la fois une sophistication croissante des modes opératoires employés par les acteurs étrangers malveillants, ainsi qu'une prolifération des attaques et campagnes exploitant l'ouverture de notre débat public numérique, dans le but de semer la confusion dans l'esprit de nos concitoyens.

En outre, l'espace informationnel est soumis aux effets indésirables des mutations du terrain numérique, notamment celles qui touchent aux plateformes en ligne hébergeant notre débat public. En effet, un nouvel écosystème numérique de l'information émerge et cherche à s'imposer progressivement. Il se caractérise par le rôle croissant des influenceurs, l'émergence de réseaux sociaux partisans et l'expansion de l'offre de médias alternatifs d'opinion, administrés par des puissances étrangères. De la même manière, l'essor de l'intelligence artificielle redéfinit radicalement les usages numériques. Elle entraîne une recomposition profonde de l'économie de l'attention et, plus précisément, de la manière dont l'information est produite, distribuée, consommée et monétisée.

Enfin, l'instrumentalisation de thèmes puissants tels que la liberté d'expression, portée par un certain nombre de dirigeants étrangers et d'acteurs économiques de la *Silicon Valley*, donne lieu à d'intenses débats culturels et politiques dans nos démocraties. La réduction des efforts de modération et de vérification des faits par plusieurs plates-formes américaines, et la rhétorique agressive employée pour dénoncer la volonté de régulation européenne participent à modeler un espace informationnel propice au développement des manipulations de l'information.

— LES PUBLICATIONS 2025 : 5 RAPPORTS, 3 GUIDES

4 FÉVRIER 2025

Manipulation d'algorithmes et instrumentalisation d'influenceurs : enseignements de l'élection présidentielle en Roumanie & risques pour la France

Afin d'anticiper la menace et préserver le débat public français des ingérences numériques étrangères, Viginum s'est intéressé et a documenté les techniques employées pour déstabiliser l'élection présidentielle roumaine de 2024, et a évalué le risque de leur transposition en France.

24 FÉVRIER 2025

Guerre en Ukraine : trois années d'opérations russes de désinformation

Depuis le 24 février 2022, l'invasion à grande échelle du territoire ukrainien par les forces armées de la Fédération de Russie s'est accompagnée d'une offensive d'envergure du dispositif d'influence informationnelle russe. Celle-ci s'inscrit dans le cadre de stratégies de « confrontation informationnelle » lancées par l'État russe dès le début des années 2000, qui ciblent la population ukrainienne et les auditoires internationaux. Son objectif est de légitimer « l'opération militaire spéciale » en Ukraine, en la présentant comme une action défensive.

12 JUIN 2025

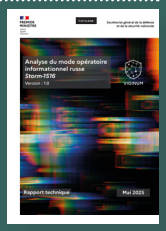
African Initiative : de la diplomatie publique aux opérations d'influence numériques

Viginum publie avec ses partenaires du *Foreign, Commonwealth & Development Office* britannique et du Service européen pour l'action extérieure, un rapport sur l'African Initiative, une agence de presse russe, pensée comme l'un des principaux vecteurs de la réarticulation du dispositif d'influence de la Russie en Afrique depuis la mort de Evgueni Prigojine le 23 août 2023. Depuis lors, les interrogations sur l'avenir des activités numériques d'influence de la société paramilitaire Wagner en Afrique sont nombreuses. Ce rapport tend à confirmer que celles-ci se poursuivent, sous une forme différente, et sont probablement intégrées au sein du dispositif d'influence informationnelle étatique russe.

7 FÉVRIER 2025

Défis et « opportunités » de l'intelligence artificielle dans la lutte contre les manipulations de l'information

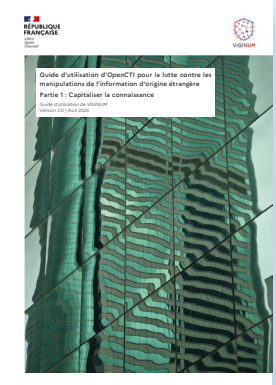
Viginum a publié un rapport, avec plusieurs partenaires internationaux, consacré aux « enjeux systémiques » liés à l'intelligence artificielle dans le cadre du sommet pour l'Action sur l'IA de 2025. Les applications d'intelligence artificielle, notamment générative (IAg), connaissent un développement spectaculaire et viennent transformer nos sociétés. L'ergonomie des produits, leur facilité d'accès et le faible coût associé ont contribué à leur adoption par le plus grand nombre.



6 MAI 2025

Analyse du mode opératoire informationnel russe Storm-1516

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 numérique francophone et européen, connu sous le nom de Storm-1516. Ce MOI, actif depuis plus d'un an et demi, est responsable de plusieurs dizaines d'opérations informationnelles ayant ciblé des audiences occidentales, dont française. Ce rapport détaille les principaux narratifs et contenus employés, leur chaîne de diffusion, ainsi que les acteurs étrangers impliqués dans la conduite du MOI.



24 AVRIL 2025
Guide d'utilisation d'OpenCTI pour la lutte contre les manipulations de l'information d'origine étrangère
À l'heure où le paysage de la lutte contre les manipulations de l'information connaît de profondes mutations, et où le nombre d'initiatives des acteurs publics et privés se multiplie, l'enjeu de l'adoption d'une grammaire commune apparaît comme essentiel.
Ce guide présente la doctrine proposée par Viginum pour répondre à ce besoin.

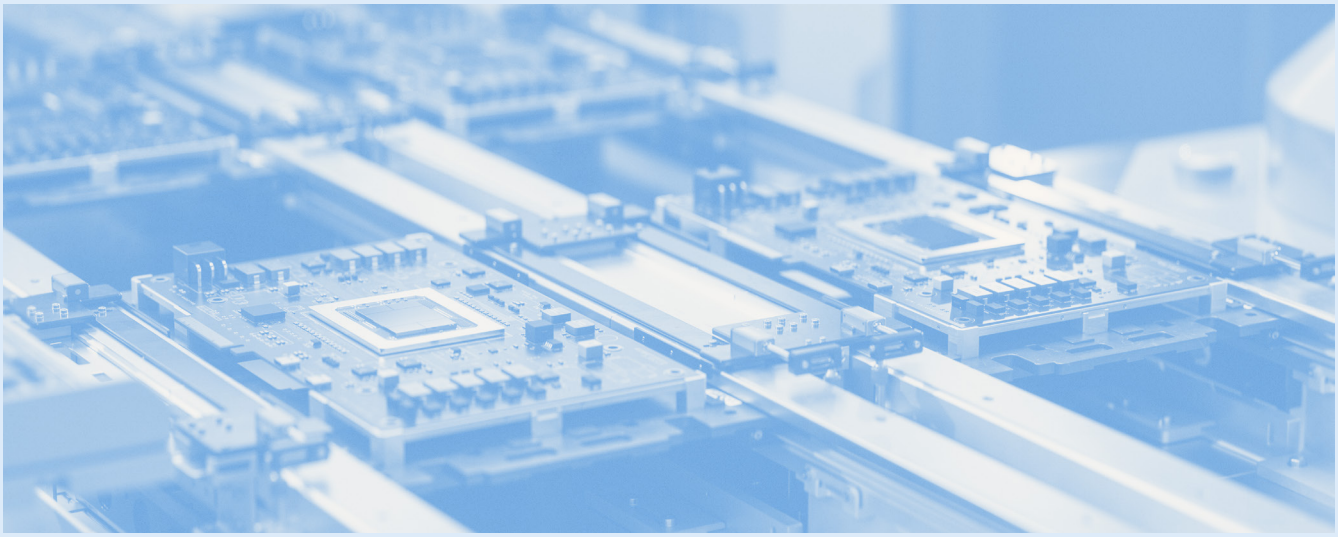
8 DÉCEMBRE 2025
Guide de sensibilisation à la protection du débat public numérique en contexte électoral
En amont des élections municipales des 15 et 22 mars 2026, Viginum a publié un guide de sensibilisation à la menace informationnelle en contexte électoral. Ce document, présenté à l'occasion du congrès de l'association des maires de France, expose plusieurs modes opératoires utilisés par des acteurs étrangers malveillants et les bonnes pratiques pour s'en prémunir.

16 DÉCEMBRE 2025
Guide de sensibilisation à la menace informationnelle à destination des acteurs économiques français
Ce guide, coécrit par Viginum et le Club des directeurs de sécurité des entreprises (CDSE), a pour objet de sensibiliser les acteurs économiques à l'existence de la menace informationnelle.
Le document présente les bonnes pratiques pour aider les entreprises à mieux détecter et réagir face aux manipulations de l'information.

— MIEUX EXPLORER LES DÉFIS ET LES POSSIBILITÉS QUE REPRÉSENTE L'INTELLIGENCE ARTIFICIELLE

Convaincu du rôle majeur que l'intelligence artificielle est amenée à occuper en matière de lutte contre les manipulations de l'information, Viginum a décidé de se doter d'une structure interne originale, tournée vers le monde de la recherche et fondée sur un objectif de partage des savoir-faire et connaissances : le centre d'excellence en intelligence artificielle. Cette structure, qui s'appuiera sur les équipes du Datalab de Viginum, aura pour missions de fournir, aux services de l'État et à la société civile, des outils pour mieux lutter contre les ingérences numériques étrangères.

Depuis deux ans, Viginum développe une activité de recherche et développement qui s'est notamment traduite par la publication d'articles scientifiques et par la participation à des conférences spécialisées. Ces travaux se sont également matérialisés par la publication, en open source, de logiciels-outils, mis à la disposition du grand public pour aider la société à mieux détecter les manipulations de l'information : d'une part l'outil D3lta, qui permet de distinguer plusieurs techniques de duplication de contenus textuels ; d'autre part un méta-détecteur, développé avec le pôle d'expertise de la régulation du numérique (PEReN) , qui facilite l'identification des contenus synthétiques diffusés sur les réseaux sociaux.



FOCUS SUR L'APPUI À LA MOLDAVIE

Depuis 2022, Viginum a mis en œuvre une stratégie d'appui au profit de pays affinitaires, dans le but de les aider à développer des capacités souveraines en matière de lutte contre les ingérences numériques étrangères. Particulièrement ciblée par la menace informationnelle russe, la Moldavie s'est dotée, dès 2023, d'un dispositif national de lutte contre les manipulations de l'information au travers du *Center for Strategic Communication & Countering Disinformation* (CSCCD).

Dans le prolongement de l'accord de coopération et de défense conclu en 2023 entre le Président de la République et son homologue moldave, Maia Sandu, une lettre d'intention a été signée le 10 mars 2025 entre Viginum et le CSCCD. Celle-ci vise à renforcer la coopération bilatérale dans le domaine de la lutte contre les manipulations de l'information et de la protection des processus démocratiques.

FOCUS SUR LA CONVENTION VIGINUM FRANCE TV

Noué le 15 octobre 2025, le partenariat entre Viginum et France Télévisions a pour objectif de mieux informer, sensibiliser et outiller le grand public face aux risques liés aux ingérences numériques étrangères.

Dans cette optique, Viginum apportera son expertise en sensibilisant l'ensemble des collaborateurs de France Télévisions lors de séances de travail et dispensera, auprès des rédactions, des formations spécifiques relatives aux modes opératoires informationnels (MOI) et aux techniques d'investigation en sources ouvertes (OSINT).

Par ailleurs, les journalistes de France Télévisions partageront leurs connaissances et leurs bonnes pratiques en matière de lutte contre les manipulations de l'information avec Viginum.

ANNE-SOPHIE **DHIVER**

Adjointe au chef du service de vigilance et de protection contre les ingérences numériques étrangères

« Nous assistons à l'émergence d'une conflictualité numérique mondiale qui s'intensifie »

Pourquoi avoir engagé un travail de rénovation du décret qui encadre l'activité du service ?

Depuis sa création en 2021, Viginum a observé une hausse significative du niveau de la menace informationnelle étrangère ciblant le débat public numérique français. Nous assistons en effet à l'émergence d'une conflictualité numérique mondiale qui s'intensifie, et dans laquelle les ingérences numériques étrangères sont devenues des instruments privilégiés au service de stratégies de puissance, mobilisés par des acteurs étatiques ou non étatiques étrangers, qui tentent d'altérer la sincérité du débat public numérique national et de peser sur les processus électoraux.

Quatre ans après sa création, Viginum a dressé un retour d'expérience de son activité et de l'articulation de ses missions opérationnelles avec le cadre juridique qui s'y applique. Défini par deux décrets (n° 2021-922 et n° 2021-1587), ce cadre nécessitait une évolution, au regard des limites opérationnelles que le service rencontre aujourd'hui face à la réalité de la menace informationnelle. Conscients de l'importance cruciale que revêt la conformité de l'activité opérationnelle du service avec le respect des libertés fondamentales, le SGDSN et Viginum ont proposé une évolution de ce cadre juridique, respectueuse du principe de proportionnalité et concertée avec les membres du comité éthique et scientifique placé auprès du SGDSN.

Quelles sont les nouvelles missions qui sont confiées au SGDSN et à Viginum ?

Le nouveau décret propose d'élargir les missions du SGDSN et de Viginum en matière de lutte contre les ingérences numériques étrangères.

Pour sa part, le SGDSN se voit doté d'une nouvelle mission d'anticipation des menaces, désormais inscrite à l'article R*. 1132-3 du code de la défense. Cet ajout doit permettre de mieux appréhender les évolutions de la menace informationnelle, notamment sur le plan technologique : intelligence artificielle, dispositifs algorithmiques, évolutions techniques des plates-formes, *etc.*

De surcroît, Viginum se voit attribuer trois nouvelles missions : une mission de « documentation de la menace », qui doit permettre de mieux capitaliser la connaissance liée aux acteurs étrangers de la menace informationnelle ; une mission de « sensibilisation » du grand public, afin de renforcer la résilience de la Nation et créer les conditions d'une immunité collective face aux ingérences numériques étrangères ; une mission de « recherche et développement », chargeant le service de concevoir des d'outils destinés à mieux détecter les opérations d'ingérences numériques étrangères, notamment afin de les mettre à la disposition de la société.

Quel effet ce nouveau décret aura-t-il sur les futurs travaux de Viginum ?

Ce projet de décret prévoit une évolution du cadre de collecte et de conservation des données pour être mieux adapté à l'état de menace actuelle et à l'évolution des usages numériques, en étendant notamment le champ d'action du service aux moteurs de recherche et aux outils d'intelligence artificielle conversationnelle. Ces modifications permettront notamment aux équipes de Viginum de suivre de manière plus efficace les modes opératoires informationnels étrangers. En outre, le rôle du comité éthique et scientifique, chargé de suivre l'activité de Viginum, est précisé, notamment en période électorale.

6

PRENDRE EN COMPTE UN ENVIRONNEMENT EN MOUVEMENT

— UN CADRE LÉGAL MAÎTRISÉ

L'année 2025 aura été celle des 10 ans du cadre législatif issu des deux lois sur le renseignement votées en 2015 et l'année du bilan de leur application. Le colloque organisé par la Commission nationale de contrôle des techniques de renseignement le 22 septembre 2025 a permis de constater que les services de renseignement avaient parfaitement intégré les exigences légales à leur travail quotidien. Le groupement interministériel de contrôle (GIC), en sa qualité d'organisme pivot pour la mise en œuvre de ces exigences, a joué un rôle essentiel dans l'appropriation du cadre légal par la communauté du renseignement.

Un autre colloque, organisé par la délégation parlementaire au renseignement, s'est tenu le 4 décembre dernier à l'Assemblée nationale avec pour objet « le renseignement français face au désordre mondial ». Le ministre de l'intérieur y a passé en revue ses attentes d'évolutions législatives pour offrir aux services des outils d'enquête plus performants dans un cadre maîtrisé.

Si le cadre légal des techniques de renseignement, posé en 2015, a été modifié à un rythme soutenu, à raison d'une fois par an en moyenne, ce fut à chaque fois l'occasion de soumettre à nouveau au débat démocratique ce régime exceptionnel, très contrôlé et indispensable à la préservation de nos valeurs et de notre autonomie dans un contexte d'incertitudes et d'intensification de la menace sous toutes ses formes.

— UNE SOLLICITATION ACCRUE

Après une année 2024 marquée par les jeux Olympiques et Paralympiques, particulièrement exigeante pour les services de renseignement et pour le GIC, il n'y a pas eu de reflux du nombre de surveillances en 2025. Le contexte sécuritaire n'a laissé aucun répit à la communauté du renseignement et le nombre de demandes de techniques de renseignement a encore augmenté.

Pour le GIC, ce surcroît d'activité se traduit de nombreuses façons : le traitement de 400 demandes quotidiennes, la multiplication des réquisitions adressées aux acteurs du numérique, l'accueil des exploitants des services de renseignement dans les locaux du GIC à Paris, en banlieue, province et outre-mer, le contrôle préalable à toute capitalisation d'informations issues des données recueillies et l'instruction des recours de particuliers. Outre sa mobilisation pour accompagner l'augmentation en volume, le GIC s'est consacré à l'amélioration des capacités offertes aux services, en modernisant ses centres utilisés par les enquêteurs, en offrant des fonctionnalités supplémentaires dans ses outils d'exploitation et en multipliant les actions de formation qu'il dispense aux agents des services.

— ALGORITHMES

Depuis 2021, le législateur a confié au seul GIC l'exécution des algorithmes. Le rapport annuel de la Commission nationale de contrôle des techniques de renseignement publié mi-2025 a consacré un chapitre entier à cette technique singulière pour en expliquer le fonctionnement et la portée.

En 2025, le GIC a poursuivi le développement de nouveaux algorithmes au profit des services dits du premier cercle, en cherchant à apporter une réponse technique à leur besoin opérationnel de détection. Le 25 juillet 2024, la loi visant à prévenir les ingérences étrangères en France[5] étendait le recours aux algorithmes à la cyberdéfense et au contre-espionnage. Le 13 juin 2025, la loi visant à sortir la France du piège du narcotrafic[6] étendait le recours à cette technique à la prévention de certaines formes de criminalité organisée. Cette loi a cependant été censurée par le Conseil constitutionnel le 12 juin, qui a aussi interdit l'accès des algorithmes aux adresses *URL*.

[5] Loi n° 2024-850 du 25 juillet 2024.
[6] Loi n° 2025-532 du 13 juin 2025.

— COMMUNICATIONS ÉLECTRONIQUES

Alors que le nombre d'autorisations d'interception de sécurité est resté stable, celui des recueils de données informatiques (RDI) a fortement augmenté. En effet, les communications électroniques interceptées auprès des opérateurs sont essentiellement chiffrées et donc inintelligibles. Si ces interceptions demeurent extrêmement utiles pour des enquêteurs car elles permettent de dresser les schémas relationnels de la personne sous surveillance, elles ne permettent que très rarement l'accès au contenu de ses échanges. La technique de recueil de données informatiques a donc été conçue pour encadrer l'accès aux données conservées en clair dans les terminaux téléphoniques et informatiques. Elle est par nature très intrusive. Afin de l'encadrer au plus juste, deux initiatives ont été lancées. L'une consiste, pour le GIC, à offrir aux services une capacité d'exploitation centralisée, sous l'œil de la Commission nationale de contrôle des techniques de renseignement (CNCTR). L'autre a pris la forme d'un ambitieux programme technique interministériel, confié au GIC avec l'appui de ses partenaires, la direction générale de la sécurité intérieure (DGSI) et la direction générale de la sécurité extérieure (DGSE), visant à assurer à la CNCTR un suivi complet des RDI en cours. Ce programme qui mobilise fortement le GIC est le premier mouvement d'une transformation profonde des outils d'exploitation du renseignement, qui bénéficiera à terme à tous les services en tirant parti des dernières technologies, grâce à un recours croissant à l'intelligence artificielle.

— RÉACTIVITÉ

Le GIC aborde avec sérénité les défis posés par les algorithmes et les RDI, tout en poursuivant son action opérationnelle au quotidien auprès des services. Ses agents répartis entre Montrouge, le quartier général historique des Invalides et quelques sites en province sont tous animés d'une même volonté de servir les intérêts fondamentaux de la Nation. Contractuels, fonctionnaires ou militaires, ils disposent de compétences variées qui sont toutes mises à contribution au sein d'une structure resserrée armée d'ingénieurs et administrateurs système et réseau, de développeurs, de spécialistes de la donnée, d'analystes de cybersécurité ou de responsables de centres de données. Le recours à des prestations et à des développements informatiques internes contribue à l'indispensable protection du secret et permet au GIC de modifier rapidement ses applications, au rythme des évolutions du cadre légal ou de la doctrine qui en découle.

— CHIFFRES CLÉS 2025

237 suppressions après constat d'anomalie

1 600 candidats aux postes techniques

7 094 comptes actifs

> 100 décisions d'habilitation

400 autorisations de techniques de renseignement par jour

55

ACCOMPAGNER LA RÉFLEXION DES AUTORITÉS

Les missions du HCEA sont définies par l'article L. 141-13 du code de l'énergie. Il s'agit notamment :

- de conseiller le Gouvernement dans le domaine de l'énergie nucléaire et de la sécurité nationale, en matière scientifique et technique, dans le domaine de la défense ou de la production d'électricité ;
- de préparer les conseils de politique nucléaire (CPN) et d'organiser le suivi de ses décisions, par délégation du SGDSN, suivant le décret du 30 décembre 2023 ;
- d'émettre des avis concernant la loi de programmation énergétique, la politique pluriannuelle de l'énergie (PPE) ou l'état des activités nucléaires civiles ;
- dans le domaine militaire, d'assurer le contrôle gouvernemental de l'intégrité des moyens de la dissuasion nucléaire ne relevant pas du ministère des armées (le CGIM) et la gestion patrimoniale des matières nucléaires nécessaires à la défense (la GPMND).

En 2025, l'action du HCEA s'est inscrite dans la continuité de l'année précédente, dans le cadre ambitieux fixé par le Président de la République lors du conseil de politique nucléaire du 17 mars 2025. Pour autant, le HCEA se doit d'adapter la conduite de ses activités à un contexte changeant. D'une part, la matérialisation progressive des craintes relatives aux approvisionnements stratégiques pose la question de la résilience du parc nucléaire face à une éventuelle rupture d'approvisionnement en uranium ; d'autre part, les périodes de prix négatifs de l'électricité au printemps 2025 et le *blackout* électrique en Espagne ont concrétisé les avertissements émis par le HCEA dans son avis de février 2025 sur la nouvelle programmation pluriannuelle de l'énergie (PPE3).

— LE CONSEIL DE POLITIQUE NUCLÉAIRE DU 17 MARS 2025

Le début de l'année 2025 a été consacré à la préparation du conseil de politique nucléaire du 17 mars 2025 puis au suivi de ses recommandations, en vue de la préparation du conseil suivant programmé en avril 2026.

Ce travail est mené en étroite collaboration avec la direction des affaires internationales, stratégiques et technologiques, avec le cabinet du secrétaire général de la défense et de la sécurité nationale et avec le secrétaire général lui-même. Il consiste à coordonner la constitution du dossier du conseil puis à suivre l'accomplissement de l'ensemble des tâches découlant de ses décisions.

Le conseil de mars 2025 a pris des décisions structurantes – deux en particulier concernent l'activité du HCEA :

- il a acté le lancement des travaux sur un programme de réacteurs à neutrons rapides valorisant l'uranium 238, permettant la « fermeture du cycle », c'est-à-dire limitant presque totalement la dépendance française aux approvisionnements en uranium ;
- il a par ailleurs donné un feu vert pour un accompagnement poussé d'un nombre restreint de projets de petits réacteurs modulaires innovants.

— TRAVAUX RELATIFS À LA RÉSILIENCE DU PARC NUCLÉAIRE FRANÇAIS

Le HCEA a mené une étude approfondie sur la résilience du parc nucléaire français, face à un scénario théorique de crise géopolitique grave, occasionnant une interruption brutale des approvisionnements de la totalité des mines de production d'uranium naturel.

Cette étude a permis d'évaluer le nombre d'années d'exploitation possible du parc nucléaire à puissance constante et de déterminer les adaptations des usines du cycle nécessaires à une meilleure résilience du parc face à une telle crise.

— TRAVAUX RELATIFS À LA FERMETURE DU CYCLE DU COMBUSTIBLE NUCLÉAIRE

Le conseil de politique nucléaire a décidé l'élaboration d'une stratégie, d'un calendrier et d'une organisation pour un programme de filière sur la « fermeture du cycle », incluant à la fois un réacteur à neutrons rapides, une capacité de production de combustible spécifique et une capacité de retraitement pour réextraire la matière et « fermer » le cycle. Le HCEA a réuni le Commissariat à l'énergie atomique et aux énergies alternatives, EDF, Framatome et Orano pour coordonner des propositions concrètes qui ont été soumises au conseil de politique nucléaire au début de l'année 2026.

Le HCEA a travaillé plus particulièrement sur les scénarios de fermeture du cycle, proposant un scénario en rupture avec les scénarios antérieurs qui visent à diminuer de 40 % le besoin de combustible à l'horizon de la fin du siècle. Il a plutôt examiné une trajectoire supprimant la consommation d'uranium externe dès 2100 et a défini les conditions d'une telle trajectoire : pilotage de la durée de vie des réacteurs du parc actuel ; conception des cœurs des réacteurs à neutrons rapides ; conception des nouvelles usines de traitement du combustible. Ces travaux aboutiront à des recommandations soumises au conseil de politique nucléaire.
Sur un thème connexe, le HCEA a mené une analyse précise sur le rythme de constitution d'un stock suffisant de plutonium pour pouvoir démarrer un parc de réacteurs à neutrons rapides et a également travaillé sur une estimation de l'éventuel coût d'échange de ce plutonium entre acteurs économiques.

LA FERMETURE DU CYCLE DE COMBUSTIBLE NUCLÉAIRE

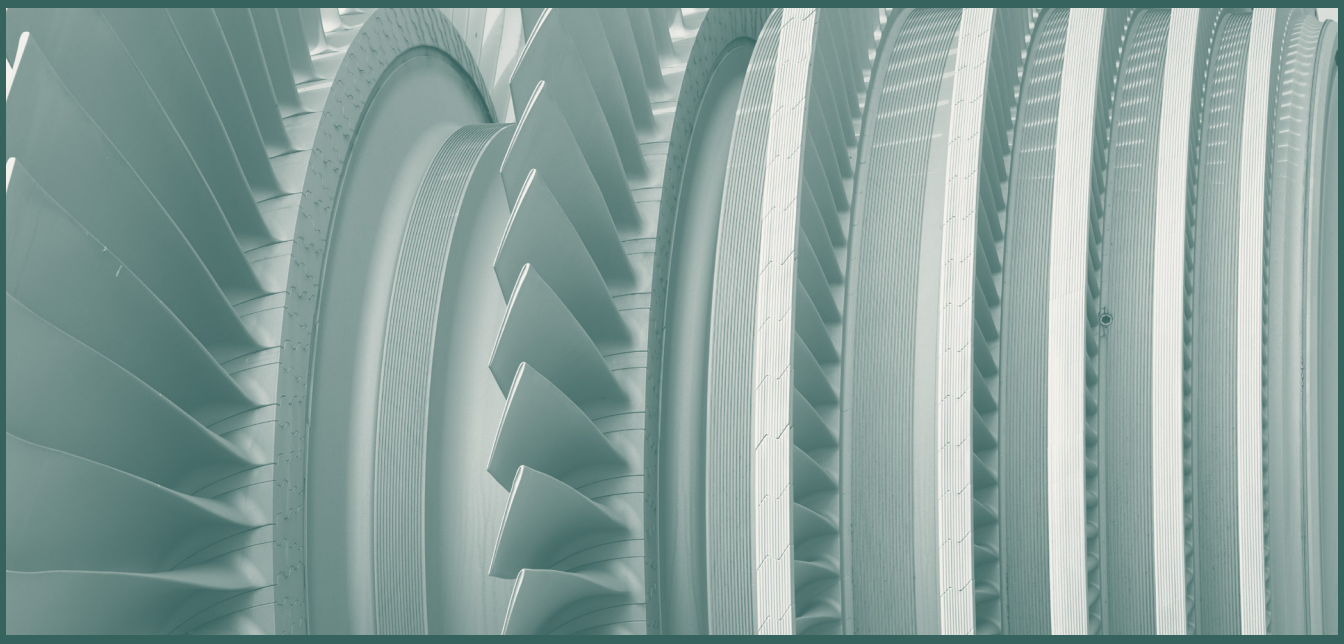
La France a choisi depuis plus de 50 ans une stratégie dite de « fermeture du cycle ». Cela signifie que le combustible usé est traité pour récupérer ses matières valorisables (uranium et plutonium), tandis que ses autres composés (produits de fission et actinides mineurs) constituent les déchets ultimes.

L'intérêt de ce choix est triple : il économise de la ressource fissile, réduit le volume de déchets ultimes à vitrifier puis à stocker et vise à diminuer la toxicité de ces stocks.

À terme, l'objectif de la fermeture du cycle est le « recyclage des combustibles usés permettant la complète valorisation des matières nucléaires et ne nécessitant aucun nouvel apport d'uranium naturel pour produire de l'énergie nucléaire. » (Orano)[7].

— TRAVAUX RELATIFS À FRANCE 2030 ET AU NUCLÉAIRE INNOVANT

Le HCEA a également mené des travaux complémentaires à son évaluation des différents projets de petits réacteurs nucléaires innovants, conduite à l'été 2024 à la demande du Premier ministre. Dans le cadre de la phase 2 du plan d'investissement France 2030, le secrétariat général pour l'investissement a associé le HCEA à l'analyse des dossiers transmis. Le HCEA a particulièrement travaillé sur les six projets de réacteurs modulaires avancés à neutrons rapides : dans ce cadre, il a analysé les perspectives de déploiement de chacune des start-ups et contribué activement à la sélection des projets.



[7] *Rapport de la commission d'enquête sur la production, la consommation et le prix de l'électricité aux horizons 2035 et 2050*, p. 673, MM. Montaugé et Delahaye, sénateurs, 2 juillet 2024.

— TRAVAUX RELATIFS À LA PPE3 ET ÉTENDUS À LA STABILITÉ DES RÉSEAUX ÉLECTRIQUES

Conformément aux termes de la loi, en février 2025, le HCEA a remis au Gouvernement un avis sur le projet de programmation pluriannuelle de l'énergie (PPE3). Cet avis était réservé pour trois raisons liées :

- la trajectoire de demande d'électricité renouvelable projetée était discutable car très volontariste à l'horizon – proche – de 2030 ;
- ces projections de forte augmentation de production d'électricité et de besoin en réseaux de transport amèneraient à une surcapacité globale, à de forts coûts additionnels, à une augmentation des prix ralentissant l'électrification et donc aboutiraient à un effet inverse de celui recherché ;
- enfin, l'obligation faite aux producteurs d'électricité nucléaire de diminuer volontairement la puissance produite (« modulation ») atteindrait des niveaux dangereux, tant pour la rentabilité économique d'EDF que pour la stabilité des réseaux.

La période du printemps 2025, d'avril à juin, a malheureusement illustré cette cascade de conséquences négatives : surcapacité de production ; prix négatifs quasi-quotidiens sur le marché européen de l'électricité ; importantes difficultés à exporter la production électrique française ; baisse de production massive de l'électricité nucléaire…

Suite à ces événements, le HCEA a développé son analyse initiale dans plusieurs documents officiels destinés au Gouvernement et au Parlement. Le HCEA a, en outre, commencé une analyse des causes du *blackout* qui a affecté la péninsule ibérique le 28 avril 2025, notamment en vue d'évaluer le risque de survenue d'un événement analogue en France.

— RÉDACTION D'UN RAPPORT D'ANALYSE SUR L'INFORMATION QUANTIQUE

Le HCEA a enfin mené en 2025 un rapport d'analyse sur l'ordinateur quantique et sur les perspectives des *start-up* françaises sur le sujet, à l'attention des acteurs intéressés par ce sujet.

VINCENT BERGER

Haut-commissaire à l'énergie atomique

« L'objectivité scientifique doit primer dans les avis confidentiels que nous remettons aux autorités politiques »

Votre travail est perçu comme un travail scientifique de haut niveau. Qu'en est-il ?

C'est pour partie vrai… mais pour partie seulement. Le fond des dossiers dont nous nous occupons peut certes toucher à des sujets scientifiques très pointus : les deux conseils scientifiques du CEA, dont j'assume la présidence, ont porté en 2025 sur la diffusion neutronique et sur l'imagerie médicale. Nous avons aussi remis un rapport d'analyse sur l'ordinateur quantique. Nous entrons aussi parfois profondément dans la physique des réacteurs pour comprendre certains projets. Mais nous passons l'essentiel de notre temps sur des dossiers d'ingénieur : l'analyse de la résilience du parc nucléaire, des trajectoires d'électrification ou l'élaboration des scénarios de fermeture du cycle ne font pas appel à une expertise scientifique poussée, ni à des outils de calcul élaborés ; juste du pragmatisme et beaucoup de règles de trois.

Ce qui confère à notre travail une qualité scientifique n'est en réalité pas le sujet traité, mais la méthode avec laquelle nous le traitons. Nous produisons, toute proportion gardée, peu de notes ; la contrepartie est que leur crédibilité doit être irréprochable. Tout chiffre est sourcé, tout jugement de valeur gratuit est proscrit, les analyses sont objectivées. Même lorsque nos résultats sont politiquement difficiles à entendre - notre avis sur la PPE par exemple -, l'objectivité scientifique doit primer dans les avis confidentiels que nous remettons aux autorités politiques. Une autre caractéristique de ce travail, par rapport à celui d'un conseiller ministériel par exemple, est le rythme dans lequel nous nous inscrivons. Il peut nous arriver de préparer une note pendant plusieurs mois.

Le SGDSN a beaucoup œuvré en 2025 pour améliorer la résilience de l'État face aux différentes menaces. Quelle a été la contribution du HCEA ?

L'essentiel de notre travail a concerné la résilience, d'une manière ou d'une autre, de notre système énergétique.

D'abord - et c'est le plus évident -, nous avons travaillé sur la question des menaces géopolitiques qui peuvent tendre, voire bloquer, soudainement le marché de l'uranium : avec une électricité produite aux deux tiers par notre parc nucléaire, la question d'une rupture d'approvisionnement complète et soudaine en uranium doit être posée. Il ne s'agit pas seulement d'en déduire qu'il faut fermer le cycle du combustible en passant aux réacteurs de quatrième génération - ce sera la réponse ultime -. Il s'agit de regarder concrètement comment s'organiser d'ici là, afin de donner aux autorités politiques la possibilité de prendre les décisions nécessaires et aux industriels le temps de les implémenter.

En regardant l'impact de notre mix de production d'électricité sur les réseaux et des trajectoires prévues dans la PPE3, nous avons aussi contribué à une vision de la stabilité des réseaux et donc à la résilience globale de notre système électrique. ▸▸▸

A quoi ressemblera votre année 2026 ?

2026 ? Une large part d'incertitude ! Comme 2025, d'ailleurs. Le Président de la République, en fonction du contexte international et du contexte industriel, va être amené à prendre de nouvelles décisions structurantes pour la filière nucléaire – sur les EPR2 (*Evolutionary Power Reactor* - Réacteur Pressurisé Européen), sur les nouvelles usines de traitement du combustible, sur la fermeture du cycle. En fonction notamment de sa décision sur le calendrier de fermeture du cycle, le travail à mener et la gouvernance à instituer prendront des formes très différentes – le rôle du HCEA également.

Il est néanmoins certain que nous continuerons à pousser nos analyses sur les usines de l'amont du cycle, afin d'accompagner les recommandations sur la résilience du parc nucléaire ; à appuyer le secrétariat général pour l'investissement sur la phase 2 de France 2030 ; à conduire des analyses indépendantes sur l'évolution du système électrique et les conséquences de cette évolution sur le parc nucléaire français. Le HCEA a par ailleurs proposé le lancement d'une revue générale sur la politique de sûreté nucléaire dans notre pays, à l'instar de la revue conduite par les Britanniques en 2025. L'enjeu pour nous est d'être capable d'accompagner, avec pragmatisme, le renouveau du nucléaire ; si une telle initiative venait à être lancée, le HCEA pourrait y participer. ◂

8

SOUTENIR L'ACTIVITÉ

ACCOMPAGNER

— RESSOURCES HUMAINES

L'année 2025 aura été caractérisée par une insuffisance structurelle des crédits de masse salariale. Pour répondre aux enjeux de gestion ainsi créés, un pilotage renforcé des ressources et la mise en œuvre de mesures d'économies ciblées ont été instaurés. Ces initiatives ont permis de préserver l'ensemble des effectifs durant le premier semestre, puis d'assurer une croissance de 30 postes à partir de l'été. Elles ont également facilité la négociation d'une dotation de crédits complémentaires, nécessaire pour absorber l'effet financier des recrutements effectués en 2024 et 2025.

La gestion du personnel civil a été particulièrement dynamique, en absorbant un flux de 310 arrivées et 290 départs, avec des délais moyens de proposition salariale inférieurs à quatre jours. Concomitamment, le processus de transformation numérique a connu une accélération, notamment par le déploiement du module informatique GAUdDI qui permet d'héberger et de consulter de manière sécurisée les documents numériques constitutifs du dossier individuel des agents et du dossier comptable, dans le respect de la réglementation et des normes archivistiques. Parallèlement, les travaux sur le module indemnitaire de RenoiRH visant à automatiser les calculs de paie se sont poursuivis. Afin d'accompagner cette modernisation, un mémento a été élaboré pour les équipes en charge des ressources humaines de proximité, garantissant une diffusion des bonnes pratiques administratives au sein des directions et services.

Ces dispositifs ont été complétés par des avancées significatives en matière de protection sociale, avec l'entrée en vigueur, au 1er janvier 2025, de la protection sociale complémentaire obligatoire garantissant une meilleure prise en charge financière de la santé des agents.

Concernant le personnel militaire, l'année 2025 a été marquée par l'achèvement de la rénovation de la cartographie des postes et par le renouvellement des conventions régissant la mise à disposition de personnels du ministère des armées et de la gendarmerie nationale. Une étape stratégique a également été franchie avec le basculement de la gestion administrative de la section de sécurité vers la Garde républicaine, mieux implantée en région parisienne, permettant ainsi de réduire les délais de vacance d'emplois du détachement de gendarmerie.

Enfin, la politique sociale est demeurée une priorité centrale de l'institution. Des actions de sensibilisation au handicap ont été menées auprès des agents, renforcées par des partenariats avec le cercle sportif de l'INI et l'association ARPEJEH pour favoriser l'insertion professionnelle des jeunes. La qualité de vie au travail a été soutenue par l'instauration d'une politique de restauration équitable sur tous les sites, ainsi que par l'organisation de moments de cohésion tels que les séminaires d'intégration et les événements de fin d'année. L'ensemble de ces progrès repose sur un dialogue social constant et constructif avec les représentants du personnel, garantissant l'amélioration continue des conditions de travail.


© SGDSN

100 %
taux d'atteinte du schéma d'emplois

+ de 31 696
jours de télétravail indemnisés

+20 ETP :
nombre d'emplois plafond créés au SGDSN (schéma d'emplois)

310
arrivées et
290
départs (agents civils, hors apprentis et stagiaires)

6 réunions du comité social d'administration

3 réunions de la formation spécialisée santé, sécurité et conditions de travail

1 330,7 **emplois travaillés** (prise en compte du temps de présence et de la quotité de travail) constatés

64

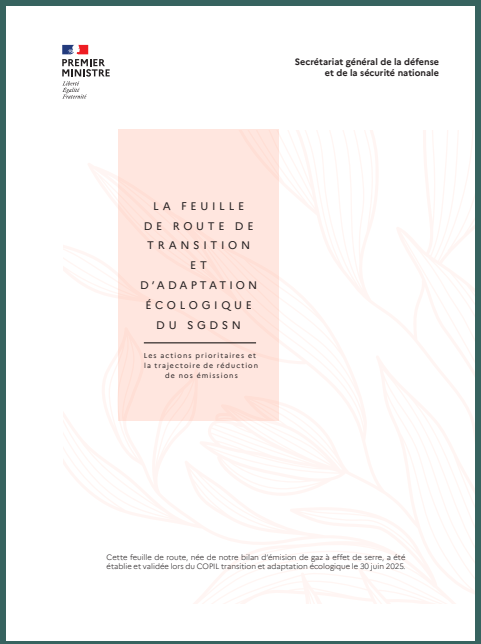
— SOUTIEN, FINANCES ET IMMOBILIER

La réorganisation de la chaine financière initiée en 2024, a produit ses pleins effets en 2025. Malgré une augmentation substantielle du budget, le cadencement des dépenses ne s'est pas ralenti, permettant une consommation intégrale des crédits. La réforme est engagée avec la fin du déploiement de Chorus Formulaire. La modernisation du processus des missions se poursuit avec la mise en place du service de démarches administratives dématérialisées *demarche.numerique.gouv.fr* tout en préservant la qualité des prestations de voyage. Afin d'approfondir la culture financière au SGDSN, le bureau des marchés a diffusé un guide de la commande publique rénové et s'est associé à la réalisation d'un programme de formation ambitieux dans le domaine financier, conjointement avec l'ANSSI.

Sur le plan immobilier, l'année a été riche en chantiers structurants. L'élaboration du projet de schéma pluriannuel de stratégie immobilière offre au SGDSN une perspective à horizon 2030. Des bâtiments modulaires de nouvelle génération ont été installés à l'été 2025 et le bâtiment 30, à l'entrée du site de l'HNI, a été rénové et accueille dorénavant des services et trois salles de réunion.

L'atelier de reprographie, déjà fortement mobilisé, a été mis à contribution dans le cadre de l'actualisation de la Revue nationale stratégique ; le bureau des archives a poursuivi la politique d'archivage permettant de classer, de verser ou de détruire les documents papier classifiés ou non, ce qui permettra d'augmenter les espaces de bureaux ; le service logistique a accompagné les autres services dans leurs évolutions et mouvements.

Enfin le SGDSN a poursuivi son engagement en faveur de la transition écologique. Après la publication d'un bilan annuel d'émission des gaz à effet de serre (BEGES), le SGDSN a déterminé 12 actions prioritaires permettant la transition et l'adaptation écologique. Des actions sont déjà engagées concernant le tri sélectif ou la réflexion sur la valorisation des déchets des équipement électriques et électroniques (DEEE) non sensibles.



© SGDSN

9 500 articles sélectionnés par le centre de documentation pour la réalisation de la revue de presse et des veilles particulières et une moyenne de 25 recherches documentaires par jour

6,11
mètres linéaires (ml) d'archives transférés au service historique des armées et 20,5 ml éliminés

Loi de finances initiale pour 2025 :
210,89 M€ (CP) en HT2 et **109,56 M€** (CP) en T2

410
opérations logistiques

6 240
ordres de mission traités

44
marchés publics lancés

5 300
opérations de maintenance réalisées

0
incident

1,8 million de tirages réalisés par l'atelier d'impression

10 509
demandes de paiement

LINE **BONMARTEL-COULOUME**

Cheffe du service de l'administration générale

« Nous devons offrir à chacun des trajectoires professionnelles lisibles et stimulantes »

Quels sont les principaux enseignements du baromètre social 2025 et comment le service de l'administration générale compte-t-il y répondre ?

L'édition 2025 révèle une adhésion croissante à la stratégie du SGDSN, soutenue par une confiance forte envers le management de proximité. Ce climat social positif repose sur une autonomie réelle et des outils de travail modernisés qui garantissent, ensemble, une qualité de vie au travail et un équilibre personnel préservés. Pour autant, nous devons encore gagner en efficacité dans nos processus de décision et la définition des responsabilités, améliorer la coopération inter-équipe et l'efficacité collective. De plus, l'année 2026 sera dédiée au renforcement des perspectives d'évolution, afin d'offrir à chacun des trajectoires professionnelles plus lisibles et stimulantes. Nous devrons également poursuivre nos efforts en matière d'action sociale et de loisirs, pour répondre aux attentes fortes exprimées dans le baromètre.

En 2025, le SGDSN a confirmé son engagement dans une politique de prévention des risques de conflit d'intérêts et d'atteinte à la probité, que pouvez-vous nous en dire ?

La déontologie désigne l'ensemble des règles et des devoirs d'intégrité professionnelle auxquels les agents publics doivent se conformer et qui répond à quatre grands principes de l'action publique : l'intégrité, la probité, l'impartialité et la dignité et ce, afin de prévenir des situations d'exposition et de se prémunir de toute mise en cause.

Les principes de déontologie applicables au SGDSN ont été rappelés aux agents, avec un point d'attention particulier sur les enjeux relatifs aux conflits d'intérêts, aux départs vers le privé, au cumul d'activité, à l'échange de cadeaux, et aux dons, avantages en nature et invitations.

Quelles sont les grandes orientations 2026 concernant l'égalité entre les femmes et les hommes ?

L'égalité entre les femmes et les hommes est une priorité constante du SGDSN. Si nos précédentes campagnes de rattrapage par les primes structurelles ont permis d'amorcer cet équilibre, l'année 2026 marquera une accélération décisive avec la transposition de la directive européenne sur la transparence salariale.

Notre ambition est de garantir une rémunération égale pour un travail de valeur égale grâce à un pilotage rigoureux. Nous finalisons actuellement un état des lieux exhaustif de nos pratiques pour identifier et corriger tout écart supérieur à 5 %. Enfin, le déploiement d'une grille de rémunération objective devra assurer une transparence totale dès le recrutement.

PREMIER
MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général
de la défense
et de la sécurité nationale

51, boulevard de La Tour-Maubourg - 75007 Paris
N 48°51'29.273'' E 2°18'36.034''
www.sgdsn.gouv.fr