PREMIER
MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

RAPPORT D'ACTIVITÉ

2024

RAPPORT D'ACTIVITÉ • RAPPORT D'ACTIVITÉ • RAPPORT

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 :
© SGDSN
© OSIIC
© GIC
© VIGINUM
© ANSSI
© Présidence de la République
© Adobestock (newafrica, doganmesut, VladislavOciacia, FlorencePiot, IMImagery, eyetronic, AUFORTJérome, bilanol, Dabarti, Dragoș Asafte, JJfoton, lovelyday12, Maximusdn, MilanNogareco, alexhitrov, rarrarorro, shintartanya)

SOMMAIRE

ÉDITO

Nicolas ROCHE

Secrétaire général de la défense
et de la sécurité nationale

Toute administration doit rendre à ses concitoyens des comptes pour l'action qu'elle mène et pour la façon dont elle remplit les missions qui lui sont confiées. C'est la première raison d'être de ce rapport d'activité du secrétariat général de la défense et de la sécurité nationale. Dans un contexte national et international à la fois intense et complexe, le temps du bilan est nécessaire pour tirer des leçons des travaux récemment menés. Naturellement, en 2024, les réalisations furent nombreuses et fortement marquées par les jeux Olympiques et Paralympiques.

Le sprint de l'été aura été précédé d'un long marathon de mesures préparatoires qui aura mobilisé un grand nombre d'acteurs, au sein de l'administration et très au-delà. Avec d'autres, le SGDSN aura rempli son rôle dans l'ensemble des domaines qui lui ont été confiés : la cybersécurité des jeux entendue au sens le plus large ; la protection des communications des autorités ; l'organisation de gestion d'une éventuelle crise ; la détection des opérations d'ingérence numérique étrangères… En complément de ces grandes fonctions, de nombreuses actions moins visibles ont aussi contribué au succès d'ensemble. On peut citer l'extension du dispositif Cynodex de détection d'explosifs aux opérateurs de sécurité privée ou la contribution du groupement interministériel de contrôle à la compréhension de l'environnement sécuritaire dans lequel s'inscrivait l'événement.

Il y a donc tout lieu de se féliciter de ce bilan, fruit du travail des agents du SGDSN, dont le professionnalisme est une nouvelle fois démontré. Il convient aussi d'en attribuer le mérite à l'investissement personnel de mon prédécesseur, Stéphane Bouillon, dont je salue l'œuvre accomplie durant les plus de quatre années passées à la tête du SGDSN. Sous sa direction, cette grande administration a continué ▸▸▸

ÉDITO

Nicolas ROCHE

Secrétaire général de la défense et de la sécurité nationale

d'évoluer, comme elle le fait depuis 1906. Sous sa conduite, le secrétariat général de la défense et de la sécurité nationale a su s'adapter en permanence à un environnement en mutation brutale et accélérée.

Cependant, le bilan de l'année 2024 ne se limite pas aux seuls JOP. D'autres missions, nouvelles ou plus traditionnelles, ont été menées à bien. Les crises Outre-mer sont venues éprouver notre organisation, notamment à Mayotte. Les conseils de politique nucléaire ont permis de mettre en œuvre une nouvelle responsabilité exercée avec le soutien décisif du haut-commissaire à l'Énergie atomique. Le travail sur les questions relatives à l'espace est venu conforter une organisation interne vouée à accompagner les ambitions de notre pays dans le domaine. Les travaux de transposition des directives européennes *REC* et *NIS2* ont permis de repenser une organisation nationale guidée tout entière par l'exigence de la résilience. Enfin, l'animation du travail interministériel a été plus que jamais au cœur de nos missions, notamment pour faire face aux modes opératoires hybrides et à l'imbrication croissante des menaces.

Nommé à la tête du SGDSN en mars 2025, j'apprécie à sa juste valeur le bilan de l'année passée. Je mesure aussi l'ampleur des défis à venir et des chantiers en cours. Annoncée par le Président de la République au mois de janvier 2025, l'actualisation de la revue nationale stratégique mobilise très largement. En la matière, le SGDSN a la responsabilité d'organiser les travaux interministériels et les consultations nationales et internationales nécessaires. L'objectif est de parvenir à une synthèse honnête et rigoureuse des basculements radicaux de notre environnement stratégique et des décisions et orientations nécessaires pour y faire face ensemble, de façon opérationnelle. C'est la Nation tout entière, dans toutes ses composantes et avec ses partenaires européens, qui devra se mobiliser.

L'enjeu est bien de nous engager pour assurer la souveraineté de la France et de l'Europe. Faire face aux menaces visibles mais aussi invisibles, avec lucidité et volontarisme. Faire face aux ruptures technologiques et savoir saisir les opportunités qu'elles présentent. Faire face à une compétition internationale dans laquelle notre industrie doit prendre toute sa place. Être fidèles aux principes fondamentaux qui sont au cœur de notre modèle démocratique et républicain.

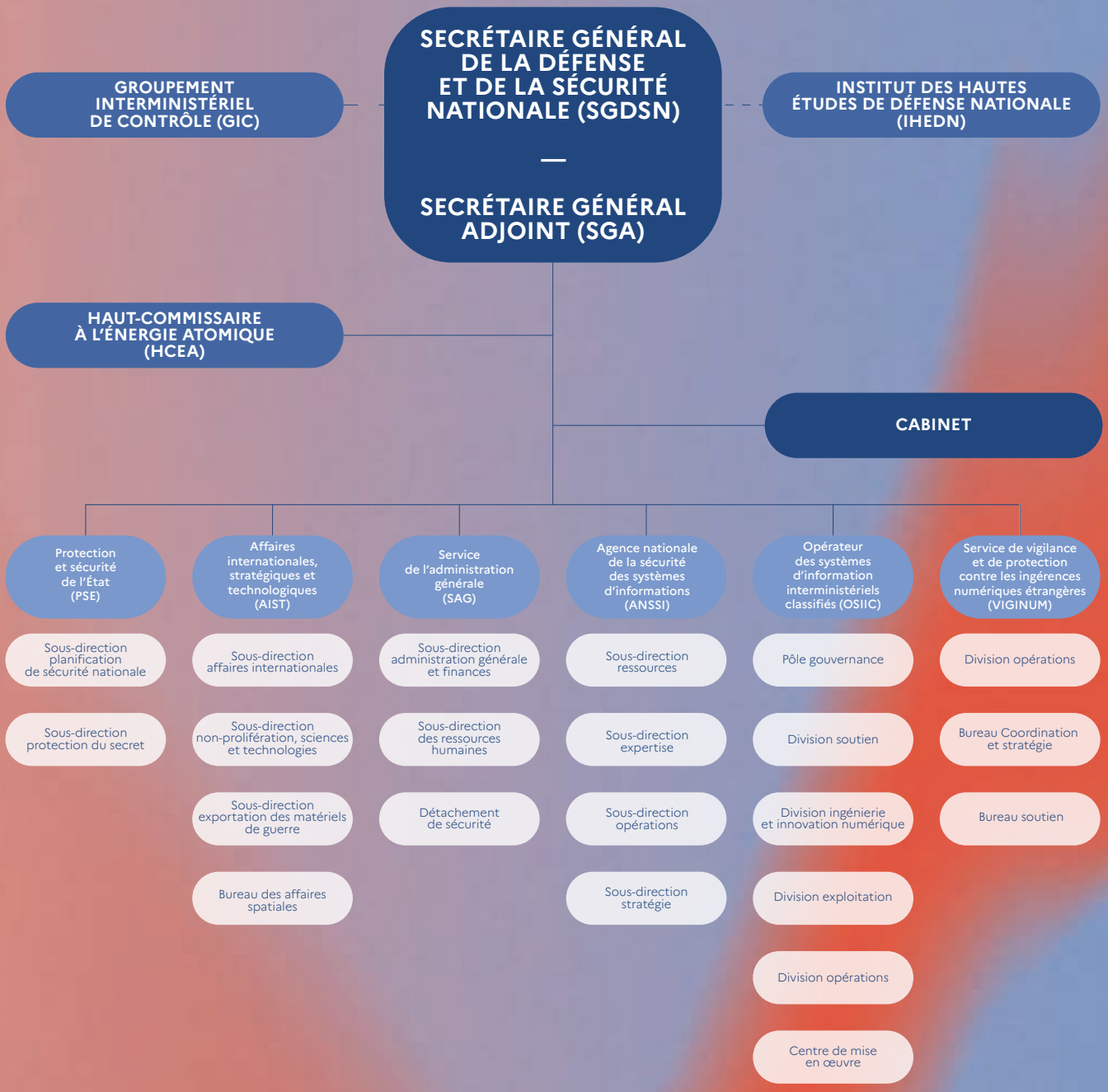
Pour sa part, le SGDSN continuera d'être concentré sur ce qui fait le cœur de sa mission : défendre au mieux les intérêts fondamentaux de la Nation.

La lecture de ce rapport vous démontrera l'engagement de notre collectif, animé par cette volonté d'anticiper, prévenir et protéger. Ces quelques pages témoigneront également de notre mobilisation toujours plus forte, sans relâche, pour notre défense et notre sécurité nationale. Au service de nos concitoyens.

Bonne lecture,

Nicolas Roche,
Secrétaire général de la défense et de la sécurité nationale. ◂

ORGANIGRAMME



Effectifs au 31/12/2024 (civils et militaires)

DIR :	31
PSE :	63
AIST :	63
SAG :	116
ANSSI :	696
OSIIC :	305
VIGINUM :	56
HCEA :	8
GIC :	302

ÉLÉMENTS DE CHRONOLOGIE 2024

9 JANVIER
Nomination de Gabriel Attal en tant que Premier ministre

15 JANVIER
Prise d'effet de la posture Vigipirate « hiver-printemps 2024 », niveau « sécurité renforcée – risque attentat »

24 JANVIER
Activation de la CIC manifestations agricoles

31 JANVIER
Dernière réunion de la CIC manifestations agricoles

1ER FÉVRIER
Inauguration du nouveau site d'entreposage de l'OSIIC

7 FÉVRIER
Dernière réunion de la CIC pénurie d'eau à Mayotte

14 FÉVRIER
Mission du Secrétaire général en Suède

22 FÉVRIER
Mission du Secrétaire général à Rennes, au sein de la zone de défense et de sécurité ouest

8 MARS
Signature de l'accord sur l'égalité professionnelle entre les hommes et les femmes des SPM

20 MARS
Mission du Secrétaire général à Washington

24 MARS
Passage de la posture Vigipirate au niveau « urgence attentat » suite à l'attentat contre le Crocus City Hall à Moscou

27 MARS
Mission du Secrétaire général à Londres dans le cadre du High-Level Group

28 MARS
Participation du SGDSN à la conférence « Usages pacifiques de la chimie et opportunités internationales » sur l'application de la Convention sur l'interdiction des armes chimiques (CIAC)

2 AVRIL
Signature d'un nouvel accord général de sécurité entre la République française et la République fédérale du Brésil relatif à l'échange et à la protection réciproque d'informations protégées et classifiées

8 AVRIL
Participation du SGA au Space Symposium aux États-Unis

2-3 AVRIL
Exercice PIRATAIR24 : anticipation des conséquences d'une crise terroriste dans le domaine aérien

7 MAI
Prise d'effet de la posture Vigipirate « été-automne 2014 », niveau « urgence attentat ». L'actualisation de la posture avait été anticipée en raison des jeux Olympiques et Paralympiques

15 MAI
Activation de la CIC évènements Nouvelle Calédonie

14 MAI
Publication du décret n° 2024-430 portant diverses dispositions relatives à la protection du potentiel scientifique et technique de la Nation

29 MAI
Mission du Secrétaire général en Ouzbékistan

C4

3 janvier
8 février
18 mars
16 avril
15 mai
17 juin
22 juillet
29 juillet
16 septembre
14 octobre
18 novembre
16 décembre

CIEEMG

18 janvier
8 février
14 mars
4 avril
16 mai
13 juin
2 juillet
12 septembre
11 octobre
14 novembre
5 décembre

CIA

22 janvier (niveau Référents)
5 juillet (niveau Dir Cab)

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

25 JUIN
Commission interministérielle de sûreté aérienne (CISA)

3 JUILLET
Exercice ORLY24 : articulation entre les transports aériens et ferrés dans le cadre d'incidents en zone aéroportuaire

25 JUILLET
Le Premier ministre Gabriel Attal s'est rendu à la Tour Mercure afin de découvrir le dispositif de sécurité des jeux Olympiques et Paralympiques de l'ANSSI

26 JUILLET
Cérémonie d'ouverture des jeux Olympiques et Paralympique de Paris, déploiement de l'OSIIC au plus près des très hautes autorités de l'État

1ER SEPTEMBRE
Le Général de corps aérien Cédric Gaudillière est nommé Secrétaire général adjoint de la défense et de la sécurité nationale

5 SEPTEMBRE
Nomination de Michel Barnier en tant que Premier ministre

6 SEPTEMBRE
Mission du Secrétaire général aux 32èmes rencontres franco-allemandes

12 SEPTEMBRE
Lancement du site de sensibilisation des élus à la stratégie nationale de résilience

21 NOVEMBRE
Mission du Secrétaire général en Italie

29 NOVEMBRE
Mission du Secrétaire général à l'OTAN

19 NOVEMBRE
Séminaire « Handicap » du SGDSN

27 NOVEMBRE
Mme Agnes Romatet-Espagne est nommée directrice des affaires internationales, stratégiques et technologiques lors du conseil des ministres

5 DÉCEMBRE
Signature de la convention de mandat avec l'OPPIC pour la rénovation d'un bâtiment de l'Hôtel national des invalides, historiquement occupé par le SGDSN

13 DÉCEMBRE
Nomination de François Bayrou en tant que Premier ministre

15 DÉCEMBRE
Activation de la CIC cyclone Chido Mayotte

19 DÉCEMBRE
Signature par le Secrétaire général de la Feuille de route stratégique 2024-2027 de l'OSIIC

COLMI

24 janvier
7 mars
22 avril
21 mai
27 juin
25 juillet
25 septembre
13 novembre
18 décembre

CIBDU

16 janvier
6 février
11 mars
2 avril
7 mai
12 juin
3 juillet
30 juillet
10 septembre
9 octobre
12 novembre
3 décembre

COLISÉ

28 février (Colisé opérationnel)
24 avril (Colisé opérationnel)
19 juin (Colisé plénier)
16 octobre (Colisé opérationnel)
4 décembre (Colisé plénier)

01

ANTICIPER, PRÉPARER ET RÉAGIR

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 (CIA) qui, depuis 2021, réunit deux fois par an une dizaine de ministères, France Stratégie et le haut-commissariat au plan. En 2024, parmi les travaux d'anticipation lancés par le CIA, quatre études majeures ont été finalisées et diffusées à la communauté interministérielle. De nature géographique ou sectorielle, les travaux d'anticipation stratégique informent les hautes autorités et préparent l'administration à différents scénarios de crise – afin de les prévenir ou d'en atténuer les effets. Ces études donnent lieu à la mise en œuvre de recommandations opérationnelles. À titre d'exemple, l'une des études de 2024 a directement permis, avant les jeux Olympiques et Paralympiques de Paris (JOP24), de consolider la sécurité de services de télécommunications satellitaires. Le CIA s'inscrit dans un renouveau de la dynamique de l'anticipation et de la prospective, observé au sein des ministères. S'appuyant également sur les apports du monde académique, de *think-tanks*, et de partenaires étrangers, la démarche d'anticipation du SGDSN participe au renforcement de la résilience de la Nation.

MENACES HYBRIDES

Dans le sillage d'une année 2023 déjà marquée par une activité soutenue de nos compétiteurs et adversaires dans le registre de la confrontation « sous le seuil armé », l'année 2024 a vu une forte hausse des attaques hybrides contre nos intérêts et ceux de nos alliés et partenaires, à la fois en nombre et en intensité. A cette augmentation de la menace répond une meilleure prise de conscience et une organisation nationale en constante évolution et toujours plus robuste, notamment grâce aux travaux interministériels animés par le SGDSN dans le cadre d'un groupe de travail permanent. Ces travaux ont permis d'évaluer, entre autres, les effets de la stratégie hybride que la Russie met en œuvre contre l'Europe, parallèlement au conflit armé en Ukraine. Ces travaux ont eu pour objectifs principaux de renforcer notre compréhension des actions de notre adversaire et notre résilience collective, mais aussi d'anticiper les menaces pouvant peser sur la France, notamment dans le cadre des élections européenne et législatives et des JOP24. Au-delà de ce seul groupe de travail, l'action centrale du SGDSN dans notre organisation interministérielle face aux stratégies hybrides en fait un acteur reconnu et un interlocuteur privilégié de nos alliés et partenaires sur ce sujet, aussi bien dans les formats multilatéraux (comme le groupe horizontal du conseil de l'UE sur les menaces hybrides) que bilatéraux. Ainsi, en 2024, le SGDSN a organisé ou participé à une quarantaine d'échanges ou évènements internationaux consacrés à la lutte contre les menaces hybrides. Enfin, le SGDSN assure l'interface entre la communauté interministérielle et la cellule de fusion hybride du centre de situation et de renseignement de l'UE. Il représente également la France au sein du centre d'excellence d'Helsinki sur les menaces hybrides, qui rassemble, depuis 2024, l'ensemble des membres de l'UE et de l'OTAN, et dont la directrice a été auditionnée dans le cadre d'une commission d'enquête par la commission des affaires étrangères et de la défense en mars 2024.

LUTTE CONTRE LES INGÉRENCES ÉTRANGÈRES

Les ingérences étrangères ont fait l'objet d'une attention particulière du Parlement depuis 2023, avec pas moins de trois rapports traitant de cette menace et formulant des recommandations. Ces travaux ont abouti au vote de la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France. Celle-ci renforce les moyens administratifs et l'arsenal répressif applicable à la lutte contre les ingérences étrangères en France, alors que des discussions sont en cours au niveau européen pour établir des mesures de transparence de la représentation d'intérêts exercée pour le compte de pays tiers. La loi instaure également des obligations de transparence renforcées par le biais d'une obligation de déclaration à la Haute Autorité pour la transparence de la vie publique - dont le non-respect est pénalement sanctionné - des personnes exerçant des activités d'influence pour le compte de puissances étrangères. Une obligation vise également un certain nombre d'organismes, dont les *think tanks* et les établissements éducatifs publics à but non lucratif œuvrant avec un partenaire étranger et ayant pour vocation la diffusion d'une langue étrangère et la promotion des échanges culturels, de déclarer les dons et versements reçus de la part de personnes morales étrangères à l'UE. Le SGDSN, qui a suivi avec une particulière attention l'élaboration de cette loi, pilote les travaux réglementaires relatifs aux deux dispositifs de transparence, dont l'entrée en vigueur est prévue au 1er juillet 2025.

ACTION INTERNATIONALE

Le positionnement du SGDSN auprès des hautes autorités politiques, et sa vision globale issue du travail interministériel, en font un interlocuteur privilégié pour nos partenaires internationaux, notamment lorsqu'ils sont dotés d'une organisation comparable à celle de la France (*National Security Advisor* ou *National Security Council*, par exemple). En 2024, le SGDSN a été de nouveau engagé sur les questions de sécurité, au sein des instances multinationales (UE, OTAN) ainsi que dans différents fora (Shangri-La dialogue, Manama dialogue…). Il a poursuivi le renforcement de plusieurs formats particuliers de dialogue bilatéraux (avec l'Australie, l'Inde, Israël, le Japon, le Qatar, le Royaume-Uni ou Singapour, notamment), dans un contexte géopolitique particulièrement dégradé où la coopération avec nos partenaires est plus que jamais essentielle. Le SGDSN 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. C'est par exemple le cas, en copilotage avec le ministère de l'Europe et des affaires étrangères, pour la stratégie Indopacifique.

LUTTE CONTRE LE FINANCEMENT DU TERRORISME

Le SGDSN a poursuivi en 2024 ses activités de coordination des administrations dans le cadre de la lutte contre le financement du terrorisme.
Le groupe de travail interministériel sur le gel des avoirs à but antiterroriste (GABAT), dont le SGDSN assure le secrétariat exécutif, a ainsi confirmé son rôle central en la matière : au 31 décembre 2024, 459 mesures de gel des avoirs pour motif de terrorisme étaient en vigueur sur le territoire national. Le GABAT regroupe l'ensemble des services et des ministères compétents, s'assure de la bonne circulation de l'information, organise et rend compte des séances de travail. Il simplifie ainsi le recours au mécanisme des gels d'avoirs visant la menace terroriste, qui ont été multipliés par 10 depuis la création du groupe en 2017. Un volet coopération internationale a été développé en 2024, suite aux recommandations du groupe d'action financière internationale (GAFI). La doctrine GABAT a été actualisée en conséquence.

EXPORTATIONS DE MATÉRIELS DE GUERRE (EMG) ET DE BIENS À DOUBLE USAGE (BDU)

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, de la défense et de l'économie. En France, l'exportation des matériels de guerre est interdite. Il ne peut être dérogé à cette interdiction que sur autorisation du Premier ministre. Cette autorisation prend la forme d'une licence d'exportation, dont l'octroi, après avis de la CIEEMG, relève du Premier ministre, et par délégation, du SGDSN. En 2024, la CIEEMG a instruit 8 200 demandes de licences d'exportation. Près de la moitié de ces demandes portent sur des modifications ou des prorogations de licences existantes. Ce chiffre témoigne d'un niveau élevé des projets d'exportation des industriels français de la défense, dans la continuité de l'activité observée depuis 2022. Une session plénière de la CIEEMG est organisée par le SGDSN chaque mois, afin de débattre des dossiers sensibles ou qui appellent un examen approfondi.

Le SGDSN est aussi investi dans l'instruction de travaux réglementaires dans le domaine de l'exportation des matériels de guerre. Dans la continuité de la parution du guide sur le traitement des exportations de biens dits « intangibles », le SGDSN a constitué un groupe de travail pour mieux encadrer les nouvelles pratiques numériques et le travail nomade, soulevant de nouveaux enjeux en matière de contrôle des exportations. Ces travaux devraient aboutir en 2025 à la publication d'un arrêté formalisant la mise en place d'une licence générale adaptée à cette évolution. Le SGDSN est également impliqué dans les échanges entretenus avec ses partenaires, au travers de différents *fora*, dont en particulier l'Accord trilatéral entre la France, l'Allemagne et l'Espagne relatif au contrôle des exportations en matière de défense, qui pourrait être élargi à d'autres partenaires européens. Enfin, au niveau 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 au règlement instituant le Programme européen d'investissement dans le domaine de la défense (EDIP).

En 2024, les membres de la CIEEMG ont été 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 de matériels de guerre, ont fait l'objet d'un traitement accéléré, afin de répondre au besoin opérationnel des armées ukrainiennes dans les meilleurs délais.

Depuis juin 2023, afin de renforcer la cohérence en matière d'exportations sensibles, le SGDSN préside également 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, le SGDSN 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. Il organise chaque mois une réunion de la CIBDU afin de débattre des dossiers sensibles ou qui appellent un examen plus approfondi. Près de 3 000 demandes de licences individuelles de biens à double usage ont été examinées en 2024. Le SGDSN a participé activement aux travaux européens d'élaboration, de mise à jour et d'application des sanctions visant la Russie et la Biélorussie. La dégradation du contexte international confirme le besoin d'un contrôle rigoureux des exportations de ces biens et technologies sensibles. Dans cette optique, le SGDSN a mené en 2024 une réflexion afin de renforcer l'efficacité du dispositif de contrôle en vigueur.

LES RÉGIMES DE CONTRÔLE AUX 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 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 intégrés dans la réglementation européenne - et des lignes de conduite.

Ces régimes, qui dépassent les logiques régionales - ils 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 sont néanmoins des piliers irremplaçables de l'architecture de sécurité internationale et leur contribution majeure à la lutte contre la prolifération s'est poursuivie en 2024 : le travail technique a ainsi permis d'aboutir à l'adoption de nouvelles propositions d'inscriptions aux listes de contrôle (1 au MTCR, 28 à Wassenaar, 1 au groupe des fournisseurs nucléaires, 4 au groupe Australie), dont plusieurs à l'initiative de la France.

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 dont l'affirmation est de plus en plus forte sur la scène internationale, à la fois grâce à leur développement économique et à une fragilisation de l'architecture de sécurité internationale.

En place depuis 2012, le dispositif de protection du potentiel scientifique et technique de la nation (PPST) a fait preuve de sa pertinence et de son utilité mais devait être adapté à cette évolution de la menace. Un travail interministériel de renforcement a ainsi été conduit, permettant d'acter la nécessité de disposer notamment d'un volet contraventionnel à la PPST et de simplifier et clarifier l'architecture réglementaire du dispositif. Cette évolution a été entérinée par la publication du décret n° 2024-430 du 14 mai 2024 portant diverses dispositions relatives à la protection du potentiel scientifique et technique de la Nation et d'un arrêté le 24 octobre 2024, confortant le dispositif dans ses objectifs de lutte contre les captations ou détournements de savoirs et savoir-faire sensibles. Cette mise à jour permet également de maintenir le dispositif français comme figure de proue européenne et internationale dans une dynamique de renforcement global de la protection de la recherche.

CONSEIL DE POLITIQUE NUCLÉAIRE (CPN)

Le discours de Belfort du Président de la République, prononcé le 10 février 2022, marque la relance du nucléaire civil français, dont la mesure la plus symbolique est un programme ambitieux de construction de six réacteurs EPR de dernière génération, avec une option pour huit réacteurs supplémentaires. Parallèlement, dans le cadre d'une approche à la fois globale et souveraine visant à « renforcer notre indépendance énergétique industrielle dans l'exemplarité climatique », une stratégie concernant l'amont et l'aval du cycle est mise en place.

Enfin, pour accompagner l'avenir, le plan d'investissement France 2030 soutient l'innovation en matière de réacteurs innovant dits *small modular reactor/advanced modular reactor* (SMR/AMR). 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 secrétariat du CPN est confié au SGDSN depuis le 1er janvier 2024, confirmant la place centrale des services du Premier ministre dans ce dossier essentiel pour la souveraineté et la sécurité économique du pays. À ce titre, le secrétaire général assure la préparation des délibérations et le suivi de la mise en œuvre des actions du CPN. Pour accompagner cette démarche, le haut-commissaire à l'énergie atomique a été rattaché au SGDSN en décembre 2023.

PARTICIPER À LA SÉCURITÉ DANS LE DOMAINE SPATIAL

L'Europe est à la croisée des chemins dans le domaine stratégique des capacités spatiales, marqué par l'émergence ces dernières années de nouveaux acteurs privés, alors que les enjeux de sécurité et de résilience autour des infrastructures spatiales sont d'autant plus importants qu'en dépendent, de façon croissante, nos économies et modes de vie.

Le bureau des affaires spatiales du SGDSN, créé en 2022, a été fortement impliqué en 2024 dans la montée en puissance du domaine spatial au niveau européen, notamment marquée par la signature en décembre 2024 du contrat de concession d'IRIS², la poursuite de l'opérationnalisation des services proposés par le programme de radionavigation et de positionnement Galileo, ou encore le projet pilote de service gouvernemental d'observation de la Terre. 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 a été mobilisé à l'occasion des discussions européennes en cours au sujet du projet d'une loi spatiale européenne, du programme spatial de l'Union européenne pour la période 2028-2034, dont le projet de règlement de la Commission est attendu au 2nd semestre 2025, ainsi que dans le cadre des réponses aux menaces hybrides en matière spatiale.

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 les activités d'instruction des demandes d'autorisation soumises par les industriels désirant travailler sur ce signal. Ce travail d'instruction a donné lieu, en 2024, aux premiers audits des acteurs industriels concernés. Cette fonction d'autorité nationale est également exercée depuis 2023 dans le cadre du programme de communications satellitaires européen (Govsatcom) et de la future constellation sécurisée IRIS², pour lesquels les travaux d'identification des potentiels utilisateurs et de leurs usages ont démarré en 2024.

Par ailleurs, la réforme de la loi sur les opérations spatiales adoptée en février 2022 a étendu le champ du contrôle exercé par le SGDSN sur les données d'origine spatiale : celui-ci ne se limite plus désormais au contrôle des seules données d'observation de la Terre par imagerie mais inclut également, entre autres, les données issues de l'interception de signaux électromagnétiques ou encore certaines données d'observation des objets spatiaux. Le SGDSN a commencé à délivrer les premières décisions sur demandes des opérateurs concernés par ce champ élargi.

L'organisation des jeux Olympiques et Paralympiques de Paris 2024 a nécessité la mise en place de mesures de protection et de vigilance accrues, y compris dans le domaine spatial. Le SGDSN a animé les travaux interministériels qui ont permis d'établir un ensemble de mesures pour assurer un niveau de sécurité renforcé de l'ensemble des services spatiaux utilisés lors des JOP.

Le SGDSN participe enfin au renforcement de la coopération dans le domaine spatial avec les partenaires américains, japonais et indiens au travers de dialogues spatiaux bilatéraux.

IRIS²

Lancé en février 2022 pendant la Présidence française du Conseil de l'UE, le programme de l'UE IRIS² vise à assurer à compter de 2030 le lancement d'une constellation de satellites pour la fourniture de services sécurisés de communication gouvernementaux. L'impulsion d'un tel projet s'inscrit dans un contexte géopolitique évolutif ayant mis en lumière les besoins croissants de l'UE en matière de communications de défense et de sécurité et l'importance de se doter de moyens souverains face à l'accélération du déploiement de l'américain *Starlink*. Multi-orbitale, cette nouvelle constellation permettra d'entrer dans la course aux grandes constellations en orbite basse dont l'UE est à ce jour absente.
Le projet s'appuie sur le principe d'un partenariat public-privé. Le consortium sélectionné, constitué des principaux acteurs européens de l'industrie spatiale et des télécommunications, comprenant notamment Eutelsat en maître d'œuvre et Airbus et Thales en sous-traitants, a signé le contrat de concession avec la Commission européenne le 16 décembre 2024. Au titre de son rôle d'autorité nationale en matière de connectivité sécurisée, le SGDSN a activement contribué en 2024 à la finalisation du corpus documentaire de l'UE fixant les exigences de sécurité du programme. Ce suivi étroit des travaux des industriels et du respect des exigences fixées doit se poursuivre dans cette nouvelle phase de mise en œuvre du contrat. Par ailleurs, le SGDSN continuera de jouer un rôle clef tout au long de la durée de vie du programme, avec l'implication de l'interministériel : gestion des demandes de services, priorisation et autorisation des utilisateurs nationaux, vérification des équipements, *etc*.

ÉCONOMIE DE GUERRE

Le 13 juin 2022, le Président de la République a déclaré au salon EUROSATORY que la France est « entrée dans une économie de guerre (…) dans laquelle nous allions devoir durablement nous organiser ». Un nouveau cap a ainsi été fixé au ministère des armées mais aussi à la base industrielle et technologique de défense (BITD) : celui de la mobilisation face au retour des conflits de haute intensité, ce qui suppose notamment d'augmenter ses capacités de production.

Pour ce faire, l'accès de la BITD au financement privé est essentiel. La Commission européenne a publié en mars 2024 une stratégie industrielle européenne de défense (EDIS) complétée d'un projet de règlement pour un programme en faveur de l'industrie de défense européenne (EDIP), qui visent à renforcer l'industrie de défense européenne par l'accroissement de la valeur des échanges intra-UE en matière de défense, et de la part des budgets d'acquisition des États européens en faveur de la BITD européenne (BITDE). Le SGDSN a pris part aux négociations relatives à ce projet de règlement.

Par ailleurs, le SGDSN contribue aux réflexions interministérielles consacrée à la problématique du financement de la BITD, qui vise notamment à anticiper les difficultés de financement (notamment des PME/ETI), à sensibiliser les instances européennes à ce besoin, à développer une culture de défense chez les acteurs du financement, à favoriser le dialogue entre le secteur bancaire et l'industrie de défense, et à adapter le cas échéant les outils de financement ou d'incitation publiques disponibles.

Pour décliner ces objectifs, le ministère des armées en lien avec la Fédération bancaire française a coordonné la désignation au sein des banques d'un réseau de référents « Défense ». De plus, l'IHEDN a mis en place dès 2023, un séminaire « Banques et industries de défense » afin de renforcer la communication entre ces deux secteurs. La deuxième édition de ce séminaire a eu lieu les 14 et 15 mai 2024. Parallèlement, plusieurs initiatives sont en cours pour favoriser les investissements de défense, y compris au niveau européen.

AGNÈS **ROMATET-ESPAGNE**

Directrice des affaires internationales,
stratégiques et technologiques

> « ... les travaux d'anticipation pilotés par le SGDSN ont notamment permis d'évaluer nos dépendances, dans une logique de désensibilisation, mais également les moyens de protéger nos intérêts stratégiques. »

Dans quelle mesure l'émergence de technologies « disruptives » a affecté le travail mené par votre direction ?

Les technologies émergentes font l'objet d'une attention croissante de la part de nos autorités en raison de leurs effets possiblement disruptifs sur nos sociétés, notre modèle économique mais aussi au regard de la protection de nos intérêts fondamentaux et stratégiques.

Les bouleversements sont d'autant plus nombreux que les technologies de ruptures, à forte dimension duale, sont diverses. Je pense naturellement à l'intelligence artificielle, en particulier aux IA génératives. On peut aussi évoquer les technologies quantiques, la fabrication additive, les biotechnologies, l'hypervélocité, ou encore les petits réacteurs nucléaires de technologie avancée (SMR/AMR).

L'ensemble de ces domaines, qui évoluent très rapidement dans un environnement compétitif exacerbé, soulèvent des questions au regard de leur potentiel proliférant. Pour cette raison, la direction assure un suivi vigilant de ces technologies et des risques associés, dans une démarche visant non pas à freiner leur développement mais à contribuer, avec l'ensemble de la communauté interministérielle à leur encadrement. L'action de la direction vise également à protéger des risques de prédation et de dissémination de nos savoirs et savoir-faire sensibles qui incluent ces technologies de rupture. Telle est par exemple la vocation de la protection du potentiel scientifique et technique de la Nation (PPST), renforcée cette année.
Au-delà de la dimension technique et de leur implication en matière proliférante, ces technologies présentent un intérêt économique, industriel et scientifique pour la Nation, et constituent de ce fait un objet de sécurité économique. Alors que nos compétiteurs stratégiques agissent de manière agressive sur ce terrain, le SGDSN contribue, au travers de notre dispositif de sécurité économique, à la protection de ces technologies dans l'intérêt national. ▸▸▸

L'année 2024 a été marquée, entre autres, par l'émergence dans les médias du sujet des câbles sous-marins. Quel regard portez-vous sur ce sujet et sur sa perception par le grand public ?

Les câbles sous-marins de communication sont des infrastructures stratégiques qui contribuent de manière déterminante au bon fonctionnement de notre pays et à la résilience de l'État. Leur importance est cruciale dans de nombreux domaines, jusque dans l'espace pour nos infrastructures spatiales !

L'importance de ces équipements explique qu'ils fassent l'objet d'atteintes dans le cadre de stratégie d'agression hybrides. Ces stratégies témoignent de la multiplicité des formes modernes de la conflictualité, au même titre que les cyberattaques ou les ingérences numériques. Tout en gardant à l'esprit que les ruptures de câbles ont le plus souvent une origine naturelle ou accidentelle involontaire, et que la redondance des câbles est la meilleure des protections, cette nouvelle menace doit être impérativement prise en compte afin de garantir la protection de nos infrastructures. Rappelons aussi que des acteurs français jouent un rôle central dans le déploiement et l'entretien de ces câbles.

Quel rôle joue votre direction dans l'anticipation des crises que nous connaissons, et dont la diversité et l'intensité se sont accrues au cours de l'année écoulée ?

Le SGDSN assure une mission de suivi et d'anticipation des crises internationales, selon une approche régionale ou thématique, notamment dans le domaine des stratégies hybrides. Il assure ce travail en se nourrissant des multiples canaux d'informations à sa disposition (notes diplomatiques ou des services de renseignements, lien avec les *think-tanks*), ou *via* le pilotage de travaux interministériels qui lui sont confiés permettant d'avoir un regard croisé sur ces sujets.
Ces travaux d'analyse sont produits pour nos hautes autorités gouvernementales, en particulier pour les Conseils de défense et de sécurité nationale dont le SGDSN assure le secrétariat, mais également au travers de travaux d'anticipation qui doivent permettre de collectivement porter nos réflexions et nos actions sur le temps long, afin de construire la résilience nationale et ne pas subir les crises. Face à l'accélération des crises que nous avons constatée en 2024, les travaux d'anticipation pilotés par le SGDSN ont notamment permis d'évaluer nos dépendances, dans une logique de désensibilisation, mais également les moyens de protéger nos intérêts stratégiques. Ces travaux sont poursuivis en 2025 dans un contexte « crisogène », alors que la revue nationale stratégique est actuellement actualisée. ◂

02

ŒUVRER EN FAVEUR DE LA RÉSILIENCE

LES JEUX OLYMPIQUES ET PARALYMPIQUES 2024 : UN TERRAIN D'EXERCICES GRANDEUR NATURE

Travail de longue haleine, la sécurisation des JOP aura mobilisé tous les services du SGDSN. Une première phase a vu plus particulièrement la direction PSE se consacrer, de janvier à mai, à l'accélération des démarches de coordination au service de la gouvernance interministérielle ou d'actions spécifiques ; une deuxième phase de suivi des évènements s'est ensuite étendue de l'arrivée de la flamme et la fin des jeux Paralympiques ; enfin une phase d'évaluation est venue clôturer ce cycle.

La préparation de l'évènement s'est concrétisée par un effort soutenu de formation des agents à la planification et la gestion de crise. Un vivier de plus de 1 500 personnes aura ainsi pu être mis en situation de répondre aux besoins de l'évènement, grâce à une démarche de professionnalisation pilotée dans la durée. L'organisation d'exercices est venue compléter cette démarche. Des exercices majeurs interministériels associant les acteurs et partenaires privés, des exercices ministériels sectoriels (télécommunication, transports, énergie, santé…) et de nombreux exercices territoriaux adaptés aux besoins locaux ont permis d'entraîner les acteurs à la communication et à la coordination interne comme externe. La prise en compte des besoins des autorités a par ailleurs conduit à élaborer des outils spécifiques d'aide à la décision, tels que le mémento pratique en matière de gestion de crise et de sécurité nationale ou le mémento de la réponse opérationnelle JOP bâti autour d'une dizaine de scénarios critiques, qui sont autant de « boites à outils » modulables synthétisant, suivant une méthode homogène, les réflexes utiles en cas de crise.

Pour la phase d'appui et de conseil aux autorités, qui s'est déroulée pendant toute la durée de l'évènement, un outil numérique - ATHENA - a permis le recueil de l'ensemble des plans gouvernementaux. Sa mise à jour collaborative, son accessibilité en cellule interministérielle de crise et l'accès intuitif aux fiches-mesures à activer ont constitué des avancées notables, opérationnelles pour les JOP. La poursuite de son déploiement au niveau territorial et son appropriation par tous les acteurs sont une priorité des prochains mois. Parallèlement, une posture Vigipirate a été spécialement élaborée pour couvrir l'ensemble de la période des JOP.

La phase de retour d'expériences et d'évaluation a été concentrée sur deux points plus particuliers. Premièrement, la gouvernance et l'articulation des centres de commandement a fait l'objet d'une attention spécifique. Le travail préparatoire minutieux effectué en amont avec tous les acteurs a ainsi contribué à la bonne appropriation de l'environnement et des procédures par les centres opérationnels. Par ailleurs le respect de la subsidiarité et la qualité des circuits d'échanges d'informations et de prises de décision ont permis de résoudre les quelques difficultés rencontrées. Deuxièmement, l'évaluation a mis en exergue l'intérêt du cycle d'expérimentations des technologies de sécurité lancé en 2019. Celui-ci aura permis de confronter des technologies d'avenir à la réalité du terrain et au cadre d'emploi. Il aura participé aux mesures des performances des technologies notamment relatives au contrôle des flux, à l'utilisation des drones, à la détection d'armes lors de tests opérationnels en conditions réelles et en comparaison d'autres moyens.

Les JOP auront globalement conforté le fonctionnement interministériel sur des sujets nécessitant une très forte coordination entre acteurs, comme la sûreté aéroportuaire et aérienne, la gestion du risque « explosifs », ou encore la gestion du risque nucléaire-radiologique-bactériologique-chimique.

4	exercices gouvernementaux notamment relatifs à la sécurité aérienne et aux transports
1 500	agents formés à la planification et la gestion de crise
5	expérimentations en situation réelle de technologies d'avenir en matière de sécurité
500	chiens formés à la détection d'explosifs

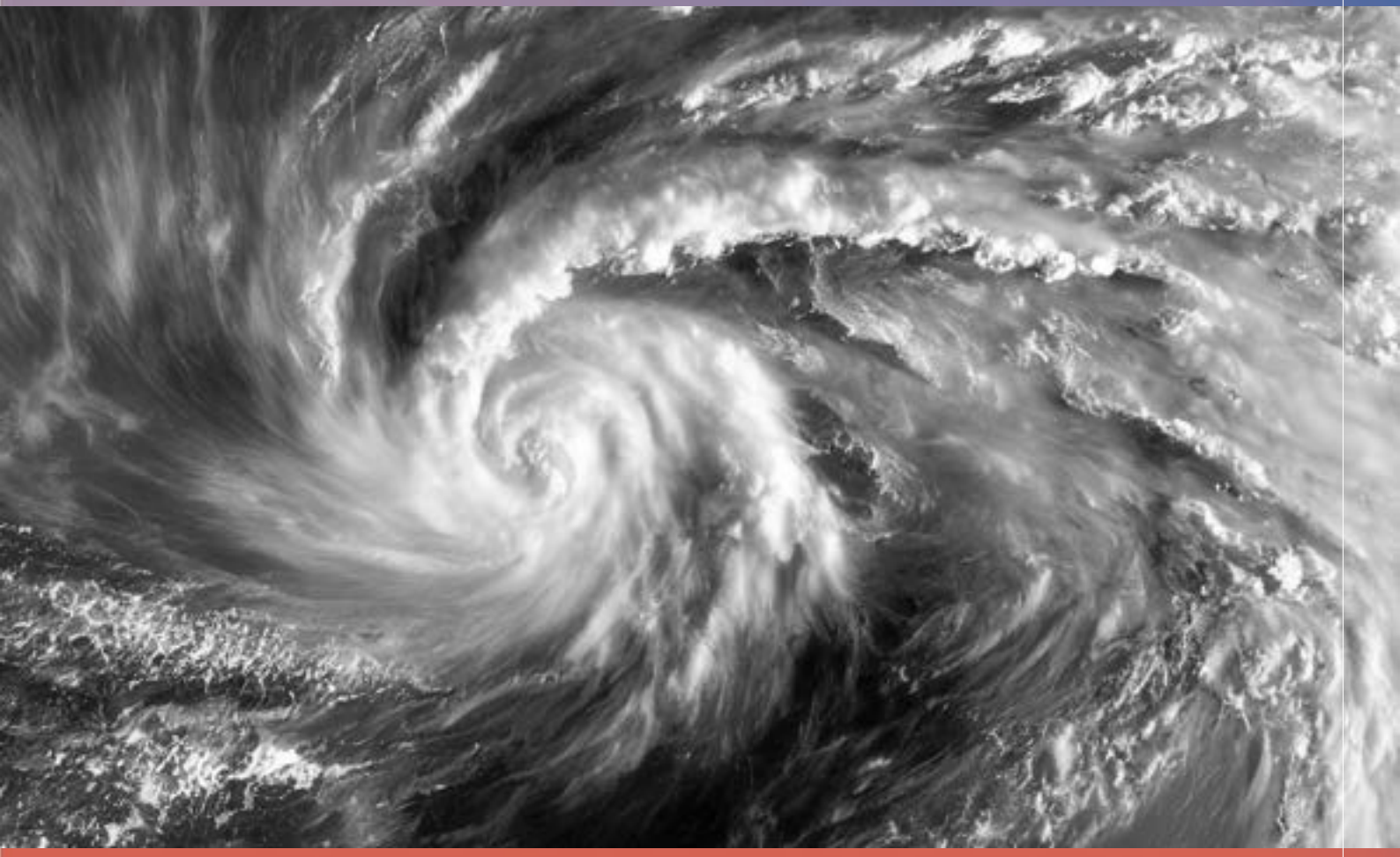
LES OUTRE-MER, ENTRE GESTION DE CRISE ET RÉSILIENCE : MIROIR ET LABORATOIRE

Les crises majeures qui ont frappé la Nouvelle-Calédonie en mai-juin puis Mayotte en décembre ont confirmé toute l'importance des travaux d'anticipation, de planification et de retours d'expérience dans le cadre des cellules interministérielles de crise (CIC) ouvertes pour la gestion et le suivi de ces évènements.

La phase de gestion de crise a notamment mis en lumière la plus-value de l'organisation interministérielle mise en place pour traiter les enjeux-clés de coordination logistique. Cela s'est notamment traduit : face à la crise de l'eau à Mayotte, avec les problématiques d'acheminement et de production d'eau ; pendant les émeutes en Nouvelle-Calédonie, par l'élaboration de scénarios potentiels de sur-crise ; ou encore après le cyclone CHIDO à Mayotte, où l'interministérialité s'est mobilisée pour élaborer des scénarios d'anticipation sur la rentrée scolaire, l'interdépendances des réseaux, la gestion des déchets… Capitalisant sur cette expérience, un séminaire sur la logistique interministérielle a été organisé en décembre 2024 par le SGDSN et le Ministère de la transition écologique et de la cohésion des territoires. Il aura permis d'exploiter les savoir-faire acquis lors des crises ultramarines et de perfectionner le fonctionnement de la cellule de coordination interministérielle dédiée à la logistique.

Si les Outre-mer sont un miroir pour les enseignements en matière de gestion de crise, ces territoires constituent aussi des laboratoires et des exemples pour le renforcement de la résilience. Les actions de formation et de sensibilisation des agents publics ont ainsi inclus un volet spécifique pour les territoires ultra-marins. Dans le cadre de la coordination de l'action du Gouvernement dans les outre-mer, le SGDN a désigné un référent outre-mer qui constituera, pour l'ensemble des services du SGDSN, le point de contact unique et privilégié pour la Direction générale des outre-mer. Il renforcera par son action, la coordination interne au sein du SGDSN pour diffuser le « réflexe outre-mer », sensibiliser l'ensemble des équipes aux enjeux ultra-marins et porter les propositions utiles en interministériel.

Les crises majeures de l'année 2024 et le fonctionnement des CIC ont ainsi confirmé l'enjeu d'une professionnalisation de la fonction anticipation/gestion de crise et le positionnement du SGDSN en appui-conseil du Premier ministre, responsable et garant de la coordination gouvernementale.



RÉSILIENCE ET SOUVERAINETÉ NATIONALES : UN ENJEU DE PRÉPARATION GLOBALE

Le durcissement du contexte géopolitique et la montée des interdépendances ont renforcé le besoin de résilience de la Nation. Un travail de recentrage opérationnel s'est opéré en 2024 autour de deux priorités validées par le Premier ministre.

Tout d'abord, a été réaffirmée la nécessité d'assurer la continuité économique de la vie de la Nation :

- garantir la résilience des réseaux essentiels : disponibilité permanente des réseaux de télécommunications, de transports d'énergie et d'eau, résilience cybernétique ;

- remédier aux vulnérabilités critiques d'approvisionnement : identification des biens vitaux pour la vie de la Nation, suivi des risques de rupture d'approvisionnement, définition des mesures de remédiation (relocalisation, diversification, stockage stratégique), repérage des capacités contributives-clés des entreprises.

Par ailleurs, l'enjeu de mobiliser, réunir et rendre utile a été réaffirmé. Cet objectif doit se traduire par :

- l'éducation, la formation et la sensibilisation aux risques majeurs à tous les âges et dans tous les territoires : introduire ces notions dans les programmes académiques, s'appuyer sur les collectivités locales et les associations pour prévenir, former et informer, élaborer un guide de la résilience à diffuser à l'ensemble de la population ;

- la constitution d'un vivier de compétences mobilisables en cas de crise majeure : garantir l'animation, l'harmonisation et l'opérationnalité des réserves, identifier et structurer l'ensemble des volontariats possibles dans les territoires, demander aux entreprises de planifier leur continuité d'activité en application de la directive européenne *REC-NIS2* dont les travaux législatifs de transposition se sont poursuivis.

Pour renforcer la résilience, au-delà des efforts déjà demandés aux opérateurs d'importance vitale et qui se sont renforcés en 2024, l'embarquement de l'ensemble des forces de la Nation est donc au cœur d'un dialogue et d'une coopération civilo-militaire qui se sont renouvelés et intensifiés en 2024 dans le cadre national comme international. Les travaux de la commission interministérielle de la défense nationale (CIDN) ont progressé autour d'un référentiel interministériel commun d'alerte et de montée en puissance (stades de défense et de sécurité nationale interministériels). Enfin l'objectif de préparation globale des Nations a constitué le dénominateur commun des échanges entre alliés au sein des instances de coopérations euro-atlantiques.

LES ÉCHANGES INTERNATIONAUX D'INFORMATIONS CLASSIFIÉES AU CŒUR D'ENJEUX ÉCONOMIQUES ET INDUSTRIELS STRATÉGIQUES

Trois années après l'entrée en vigueur de la réforme de la politique de protection du secret de la défense nationale, le SGDSN a renforcé en 2024 l'animation de son réseau de fonctionnaires de sécurité - défense et relancé l'animation semestrielle des correspondants du réseau national OTAN - UE. Il a également accompagné les ministères dans la déclinaison de la nouvelle version de l'IGI 1300 et a poursuivi ses travaux d'élaboration de fiches pédagogiques à destination des responsables d'organismes et des bureaux de protection du secret. Dans ce souci d'un meilleur accompagnement des utilisateurs, des travaux ont été lancés pour l'élaboration d'un parcours numérique à destination des personnes habilitées. De même, le projet visant à dématérialiser la procédure, la gestion et le suivi des habilitations afin d'en accélérer et d'en sécuriser le traitement s'est poursuivi dans un contexte budgétaire et technique complexe.

Par ailleurs, la sous-direction de la protection et de la sécurité de la défense nationale a intensifié sa mission de contrôle de l'application de la réglementation nationale, européenne et otanienne, ainsi que du niveau de protection des informations les plus sensibles. Sur le plan international, la révision des accords généraux de sécurité (AGS) a été une priorité de l'année 2024 avec la montée en puissance du bureau des affaires internationales et européennes (BAIE) et l'élaboration d'un processus de priorisation et de dynamisation des négociations, en lien étroit avec les acteurs interministériels. Les premiers résultats sont au rendez-vous avec la signature d'un nouvel AGS avec le Brésil en avril 2024 et la négociation active en parallèle de neuf accords (avec l'OCCAR ; l'Allemagne ; l'Italie ; le Royaume-Uni ; les Pays-Bas ; l'Inde ; l'Ukraine ; le Portugal ; Singapour).

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

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

4 200 décisions d'habilitation délivrées par la sous-direction PSD dans son périmètre de compétence

MURIEL **NGUYEN**

Directrice de la protection
et de la sécurité de l'État

« Face à des menaces qui ne sont plus seulement militaires, c'est l'ensemble de la Nation qui doit se défendre. »

La direction PSE exerce des missions interministérielles par nature. Comment cela se traduit-il concrètement ?

En effet, il s'agit bien d'un positionnement spécifique en administration centrale qui consiste à animer, impulser, coordonner l'action des ministères sans s'y substituer, tout en sachant se montrer incitatif et volontariste. Cette capacité de conviction s'appuie sur une expertise et une maîtrise technique et pluridisciplinaire des questions de défense et de sécurité nationale, alliée à une appréhension des enjeux politiques et des équilibres institutionnels qui sont omniprésents dans ces matières. Quotidiennement, notre action bénéficie du réseau des hauts fonctionnaires de défense et de sécurité des ministères qui constituent des relais très actifs, réactifs et polyvalents, mobilisés sur tous les fronts malgré des ressources comptées. Dans le contexte actuel, difficile, j'ai le sentiment que les ministères et au-delà l'ensemble des opérateurs, ainsi que nos partenaires publics et privés dans leur diversité, peuvent trouver au SGDSN un espace de travail en confiance, dans une interministérialité constructive.

Quelles sont les missions qui montent en puissance ?

Notre modèle évolue. L'état de la menace exige une préparation permanente et des adaptations continues. La réponse gouvernementale s'adapte par paliers successifs et réversibles. Nous avons besoin d'une boite à outils interministériels très souple pour mettre en cohérence l'ensemble des efforts et réagir collectivement selon des schémas coconstruits en amont des crises. C'est le sens du travail engagé avec l'ensemble des acteurs publics et privés pour une coopération civilo-militaire renforcée.

On parle beaucoup de résilience mais dans quel sens orientez-vous vos actions ?

L'idée générale peut-être résumée ainsi : face à des menaces qui ne sont plus seulement militaires, c'est l'ensemble de la Nation qui doit se défendre, toutes les ressources sont utiles et le soutien civil est essentiel. Les priorités et des actions concrètes ensuite : nous opérationnalisons la stratégie nationale de résilience autour, d'une part de la continuité des réseaux et des approvisionnements essentiels, d'autre part de l'implication citoyenne car rien ne peut se faire sans les ressources humaines et morales du pays.

03

RENFORCER LES CAPACITÉS DE L'ÉCOSYSTÈME

UNE CYBER-MENACE STABLE MALGRÉ DES OCCASIONS D'ATTAQUES

En 2024, les cyberattaquants ont saisi un ensemble de possibilités qui s'offraient à eux, qu'elles soient conjoncturelles (jeux Olympiques et Paralympiques 2024, élections, tensions internationales, *etc.*), structurelles – *via* par exemple le ciblage de la chaîne d'approvisionnement des entités visées – ou techniques, comme en témoignent les campagnes d'exploitation massive de vulnérabilités affectant certains équipements de sécurité placés en périphérie des systèmes d'information. Plus de la moitié des opérations de cyberdéfense de l'ANSSI en 2024 ont ainsi eu pour origine l'exploitation de vulnérabilités sur ces équipements, devenus des cibles de choix des attaquants.

L'ANSSI est donc demeurée fortement mobilisée par la réponse aux attaques à but d'espionnage, caractérisées cette année par le ciblage accru d'équipements et d'infrastructures de télécommunications. L'utilisation continue de réseaux d'anonymisation[1] par les attaquants leur permet de dissimuler leurs actions et en rend l'attribution difficile, à toutes les étapes de l'attaque informatique. L'essor des entreprises privées de lutte informatique offensive permet quant à lui le développement de capacités parfois très sophistiquées qui ne sont plus uniquement le strict apanage des États, et le ciblage d'organisations *via* les équipements mobiles de leurs employés, souvent situés en dehors ou en marge des systèmes d'information protégés.

La menace cybercriminelle – fortement industrialisée ces dernières années – constitue désormais un risque systémique pour les organisations françaises. Elle se caractérise principalement par des fuites de données et des attaques par rançongiciel, dont le nombre traité par l'ANSSI s'est stabilisé à un niveau élevé depuis 2023.

Enfin, en 2024, l'ANSSI a constaté une hausse des attaques à finalité de déstabilisation, notamment opérées par des groupes « hacktivistes » privilégiant les attaques peu sophistiquées, comme les interdictions de service (*DdOS*).

LES JEUX OLYMPIQUES ET PARALYMPIQUES 2024 SANS CYBERINCIDENT MAJEUR

En raison de leur rayonnement mondial, les jeux Olympiques et Paralympiques 2024 étaient susceptibles d'attirer l'attention de divers acteurs cybermalveillants cherchant à profiter de cet évènement pour acquérir une certaine visibilité et faire connaître leurs revendications, attenter à l'image et au prestige des compétitions comme à ceux de la France ou tout simplement chercher à obtenir des gains financiers par extorsion.

Face à cette menace, l'ANSSI assurait le pilotage de la stratégie de prévention des cyberattaques des jeux Olympiques et Paralympiques, en étroite collaboration avec les différentes structures impliquées dans l'organisation des jeux – dont en particulier la délégation interministérielle aux jeux Olympiques et Paralympiques, le ministère de l'intérieur et des outre-mer et le comité d'organisation des jeux Olympiques et Paralympiques (Paris 2024).

La pleine mobilisation des agents, la préparation des parties prenantes aux JOP et le dispositif opérationnel spécialement mis en œuvre ont permis qu'aucun évènement cybersécuritaire n'affecte les cérémonies d'ouverture et de clôture ou les épreuves. Si un total de 548 évènements de cybersécurité a été recensé par l'ANSSI entre le 8 mai, date de l'arrivée de la flamme à Marseille, et le 8 septembre 2024, date de la cérémonie de clôture des jeux Paralympiques, leur effet sur le déroulement de l'évènement a été faible ou nul.

Les jeux ont ainsi permis à la France de démontrer sa résilience en matière de cybersécurité, à l'écosystème cybersécuritaire national de renforcer ses capacités de coordination et d'action commune et à l'ANSSI de mettre en place un cadre pérenne pour la gestion de crise majeure.

[1] Réseaux constitués d'équipements compromis par un attaquant qui en détourne l'utilisation légitime pour mener ses opérations plus discrètement.

LA PRÉPARATION DE LA TRANSPOSITION DE LA DIRECTIVE *NIS2*

Adoptée en décembre 2022, la directive européenne sur la sécurité des réseaux et des systèmes d'Information (*NIS2*) vise à améliorer la cybersécurité de l'ensemble des acteurs de notre économie et de nos services publics en imposant des règles de sécurité informatique harmonisées. Elle a pour objectif d'atténuer les menaces pesant sur les réseaux et les systèmes d'information fournissant des services essentiels dans les secteurs clés et d'assurer la continuité de ces services en cas d'incident.

La transposition en droit national a débuté en octobre 2024 avec l'adoption d'un projet de loi par le Conseil des ministres. Le projet a été adopté par le Sénat le 12 mars 2025. Il poursuivra son parcours, à l'Assemblée nationale durant le mois de mai.

Parallèlement, l'ANSSI travaille à l'accompagnement des futures entités régulées pour faciliter leur compréhension de la règlementation et les soutenir dans la mise en œuvre des obligations auxquelles elles seront assujetties, en développant l'offre de services et assurant une coordination renforcée avec les différentes parties prenantes.

4 386	évènements de sécurité
1 361	incidents
280	visas de sécurité délivrés
196	qualifications
94	certifications
117 856	attestations SecNumacadémie délivrées
1 696	personnes formées
68	formations labellisées SecNumedu
35	formations labellisées SecNumedu-FC
22	articles scientifiques publiés
1	avis technique publié
10	guides techniques publiés
12	logiciels publiés en *open source*

VINCENT STRUBEL

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

> LES JEUX ONT CONSTITUÉ L'ABOUTISSEMENT D'UN TRAVAIL ACHARNÉ DE SÉCURISATION D'UN ÉCOSYSTÈME VASTE ET ÉCLECTIQUE

Quels évènements vous ont le plus marqué en 2024 ?

Je ne vais pas vous surprendre : l'activité de l'ANSSI en 2024 a été considérablement marquée par les jeux Olympiques et Paralympiques de Paris. Pour l'Agence, les jeux ont constitué l'aboutissement d'un travail acharné de sécurisation d'un écosystème vaste et éclectique. Cela aura été pour nous une sorte de 100-mètres, mais qui aura duré deux ans ! Cet épisode hors-norme nous a mis à l'épreuve comme jamais auparavant, tant en matière de prévention que de réaction et ce, à grande échelle. Je considère en effet que jusqu'à 30 % de notre force de travail aura été mobilisée par les jeux. Notre aptitude à impliquer et à coordonner une multiplicité d'acteurs aura aussi été grandement challengée. Le principal enseignement à retirer à l'issue – et c'est une bonne nouvelle - est que nous avons relevé ces défis avec succès, puisqu'aucun attaquant n'a réussi à perturber le déroulement de l'évènement, en dépit de nombreuses tentatives !

D'autres défis nous ont également occupé cette année. Je pense en particulier à la sécurisation des deux grands rendez-vous électoraux nationaux successifs qu'ont été l'élection européenne et les élections législatives, en juin et juillet. Il s'agit toujours de moments particuliers de vigilance pour nous, compte tenu de l'importance qu'ils revêtent dans la vie institutionnelle de notre pays.

Nous avons par ailleurs mené de nombreux chantiers visant à faire évoluer le cadre de l'action de l'ANSSI. Je pense en particulier aux travaux liés à la transposition en droit national de la directive européenne NIS2, texte essentiel qui permettra de renforcer la sécurité de plusieurs milliers d'entreprises et d'administrations de notre pays.

Une autre grande avancée a été l'adoption, en octobre, par le Conseil de l'Union européenne, du Cyber Resilience Act (CRA). Ce texte, qui généralise à l'ensemble des produits numériques des exigences d'hygiène numérique, complète la directive NIS2 en répartissant l'effort de cybersécurité entre fournisseurs et utilisateurs.

Comment l'Agence s'est-elle préparée à cet élargissement du cadre de son action ?

Nous travaillons à cette évolution depuis plusieurs années. Des étapes importantes ont à nouveau été franchies en 2024. Je pense en particulier à la nouvelle emprise de l'ANSSI localisée à Rennes, qui vient de vivre sa première année complète et a pleinement rempli sa promesse de renforcer les synergies avec l'écosystème public et privé déjà implantés dans le bassin rennais – place forte de la cybersécurité ! – et la région Bretagne dans son ensemble.

Je pense également à l'aboutissement des travaux de préfiguration de la nouvelle mission de contrôle et de supervision conférée à l'ANSSI. Au travers de l'aspect dissuasif d'éventuelles sanctions prévues par plusieurs textes législatifs, cette mission complètera l'accompagnement, le conseil et l'assistance assurés depuis toujours par l'ANSSI, dans le même objectif de renforcement du niveau de cybersécurité de la Nation.

Quels sont les éléments clef de votre feuille de route 2025 ?

Parmi ses chantiers, l'ANSSI aura à cœur de poursuivre le développement de son expertise sur les nouvelles technologies à fort enjeu de cybersécurité, en particulier l'intelligence artificielle et la cryptographie post-quantique, avec sur ce thème la définition d'un plan national de transition, pour disposer de mécanismes de sécurité adaptés à la perspective de l'ordinateur quantique.

Dans la continuité des efforts entrepris ces dernières années pour permettre de couvrir un champ d'acteurs toujours plus large, l'ANSSI s'attachera également à mettre en œuvre la directive *NIS2*, en concertation avec les futures entités régulées et les fournisseurs de services, et en accompagnant au mieux les organisations concernées. Il sera par ailleurs essentiel de poursuivre les travaux de clarification de notre offre de services, en construisant des parcours cohérents pour les entités régulées et non régulées en lien avec les acteurs de l'écosystème de cybersécurité. Tout cela se fera avec le souci de communiquer toujours plus efficacement, pour partager nos recommandations sur les enjeux et évolutions structurantes du paysage numérique.

04

FIXER LE CAP

L'OSIIC FIXE LE CAP POUR LES TROIS ANNÉES À VENIR

Depuis sa création le 1er juillet 2020, l'OSIIC a mené de nombreux chantiers, principalement à des fins d'innovation ou de rationalisation. Jeune service à compétence national, l'OSIIC a également, au cours des dernières années, œuvré à stabiliser ses effectifs, consolider son organisation et repenser ses relations avec ses différents bénéficiaires. Afin de répondre aux besoins exprimés par les plus hautes autorités de l'État, par la communauté interministérielle ou encore par les agents du SGDSN, l'OSIIC a mené de nombreux chantiers d'ampleur en parallèle.

L'année 2024 aura été marquante à plusieurs titres. D'une part, comme pour tous, l'année passée aura été une année olympique, synonyme d'exigence, d'excellence et d'esprit sportif ; d'autre part, elle a été l'année du dévoilement de la feuille de route stratégique 2024-2027 de l'OSIIC, fruit d'un travail collaboratif, constituant un cadre ambitieux pour les prochaines années, à la hauteur des défis de l'époque.

En effet, dans un contexte de menace stratégique renforcée, offrir des services de très haute sécurité exige un effort continu et une attention de tous les instants.

OFFRIR DES SERVICES RÉNOVÉS ET SÉCURISÉS

Dans une optique d'excellence opérationnelle et de renforcement de la cybersécurité, d'importants projets de modernisation des systèmes d'information ont abouti en 2024. Capitalisant sur la modernisation du téléphone portable Secdroid, menée de concert avec le ministère de l'intérieur dans le cadre du partenariat NEO2, l'OSIIC a mis en service une nouvelle gamme de terminaux auprès de l'ensemble des 1 100 utilisateurs du SGDSN. Pour sa part, le ministère de l'intérieur à mis en service 236 000 terminaux sécurisés auprès des forces de sécurité intérieures depuis 2022, sous l'égide de son agence numérique.

L'OSIIC a par ailleurs contribué à une déclinaison de Secdroid sur 23 000 tablettes « multi-utilisateurs », permettant ainsi d'équiper les réservistes de la police et de la gendarmerie d'outils de mobilité.

En outre, l'offre de téléphonie mobile sécurisée apte à protéger toute information sensible non-classifiée a été renforcée et pérennisée. Ce réseau fermé dessert environ 700 utilisateurs au sein du Gouvernement et de l'administration.

Enfin, l'année 2024 a été marquée par des travaux de rénovation et de modernisation des réseaux classifiés, avec le déploiement du bureau numérique secret au profit de l'ensemble des bénéficiaires de l'OSIIC. Dans un double objectif de sobriété énergétique et budgétaire, un effort important a également été engagé pour rationaliser le parc informatique en retirant du service les terminaux obsolètes ou redondants.

Pour répondre aux besoins croissants des utilisateurs et améliorer les conditions d'utilisation, les capacités des réseaux ont été significativement augmentées. Ainsi la capacité de stockage a été doublée lors de sa migration.

GARANTIR UNE PERFORMANCE OPÉRATIONNELLE OPTIMALE

Comme l'ensemble du SGDSN, l'OSIIC a été très mobilisé avant et durant les jeux Olympiques et Paralympiques de Paris 2024. Le bon fonctionnement des systèmes qu'il administre a permis à l'ensemble des parties prenantes, notamment interministérielles, de se préparer au mieux à cet évènement et d'en sécuriser le bon déroulement.
Un effort particulier de déploiement des réseaux classifiés à haute disponibilité a été consenti afin de desservir l'ensemble des acteurs devant y avoir accès dans le cadre des JOP 2024.
De plus, le réseau de travail quotidien du SGDSN a fait l'objet d'une rénovation majeure, afin d'en renforcer substantiellement la disponibilité pour faire face à l'éventualité d'une opération de gestion de crise. Les travaux menés sur cette infrastructure, entamés dès 2023, se sont poursuivis en 2024 et ont été validés lors d'un exercice de télétravail généralisé au printemps.
En parallèle, l'OSIIC s'est mobilisé pour équiper au mieux le SGDSN, afin qu'il dispose de tous les outils nécessaires dans le cadre de la mission qui lui était confiée pour assurer la sécurité des JOP. Les salles de crise ont ainsi été équipées de moyens propres et les agents de l'ANSSI recrutés pour l'évènement ont été dotés d'équipements adaptés.
Le travail préparatoire effectué très en amont a permis à l'OSIIC d'allier réactivité et agilité. Les agents de l'opérateur ont de surcroît assuré une présence opérationnelle à plus de 70 % des effectifs durant toute la période des JOP.
L'OSIIC a également accompagné les changements de Gouvernement en déployant très rapidement ses moyens sécurisés auprès des nouveaux ministres et des membres de leur cabinet.
Indépendamment des évènements exceptionnels, la mobilisation des équipes de l'opérateur a été tout aussi remarquable lors des déplacements des très hautes autorités de l'État (THAE). Mission centrale de l'opérateur, héritée du centre des transmissions gouvernementales, l'OSIIC installe et met en œuvre ses moyens de communication hautement sécurisés au profit du Président de la République, du Premier ministre et de certains ministres, dans des contextes opérationnels complexes. En 2024, les équipes de l'OSIIC ont préparé et accompagné 24 voyages officiels du Président de la République et assuré les communications sécurisées durant 300 heures de vol de l'avion à usage gouvernemental (AUG).

UN NOUVEAU CHAPITRE POUR L'OSIIC

L'année 2024 marque un tournant pour l'OSIIC qui entame une nouvelle phase de son développement, matérialisée notamment par sa feuille de route stratégique 2024-2027.

Un important travail collectif de consultation interne a été mené, puis une démarche comparable a été conduite auprès des très hautes autorités de l'État, des ministères et du SGDSN, afin que tous les bénéficiaires des services de l'OSIIC puissent contribuer à la définition des chantiers majeurs de l'organisme pour les trois prochaines années.

L'OSIIC se dote ainsi d'une stratégie numérique pour soutenir la décision et l'action interministérielles dans un contexte de compétition stratégique accrue. Cette ambition s'articulera autour de quatre axes.

Conforter son rôle d'opérateur interministériel de systèmes et services numériques de très haute sécurité

Cet axe traduit plusieurs ambitions. En cohérence avec son positionnement interministériel, l'OSIIC se doit de soutenir une fluidification des échanges classifiés, à très haut niveau de sécurité, au profit des politiques de protection des intérêts fondamentaux de la Nation, face aux menaces hybrides.

Dans un contexte de transformation numérique continue, les cyberattaques sont aujourd'hui des menaces stratégiques majeures. C'est pourquoi l'OSIIC se doit de mettre en œuvre les pratiques de cybersécurité les plus modernes. Pour ce faire, il s'appuie sur un partenariat renforcé avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui apporte son expertise technique et sa connaissance de la menace à l'OSIIC. Ces échanges se sont révélés particulièrement pertinents durant les JOP2024 afin de garantir la sécurité et la résilience des systèmes d'information de l'État.

Concevoir, déployer, maintenir et exploiter des systèmes à l'état de l'art

Dans une démarche d'amélioration continue et d'optimisation de la performance opérationnelle, l'OSIIC compte regagner en liberté de manœuvre pour remplir ses missions à moindre effort et à moindre coût, en se rapprochant des meilleurs standards, tout en renforçant la robustesse de son dispositif interne.
L'opérateur prend désormais en compte les aspects d'éco-conception tout en s'adaptant aux spécificités des éléments les plus sensibles afin de garantir la sécurité nationale. Cette action doit être réalisée pour tous les systèmes administrés, tout en s'adaptant aux spécificités des éléments les plus sensibles afin de garantir constamment la sécurité nationale. Cela se traduira *a minima* par une analyse de l'impact environnemental des choix réalisés et un effort partout où les analyses de risques le permettent, en particulier sur les systèmes non classifiés.

La satisfaction des utilisateurs au cœur

Le sens du service et la satisfaction des utilisateurs composent l'une des trois valeurs historiques de l'OSIIC. Le niveau de satisfaction des utilisateurs recherché impose de s'assurer de la simplicité et de l'efficacité des activités de soutien qui devront être organisées en partenariat avec des acteurs de proximité et dont la performance devra être mesurée.

Attirer, fidéliser et accompagner les talents

Dans un marché du travail numérique très disputé, l'OSIIC doit attirer les compétences tout en fidélisant et accompagnant dans leurs évolutions professionnelles les agents déjà en poste. L'OSIIC dispose en son sein de métiers uniques et atypiques requérant des expertises spécifiques. En 2024, soucieux de les faire connaître, l'opérateur a accueilli 8 stagiaires post-bac, 19 stagiaires en observation (collégiens et lycéens) et 10 apprentis. Cet effort est consenti par les agents de l'OSIIC, passionnés et soucieux d'accompagner et former les étudiants ou futurs étudiants souhaitant travailler dans les métiers du numérique.

CHIFFRES CLÉS

30 M€	de budget annuel par an
1 300	utilisateurs au sein du SGDSN
1	assistance joignable 24h/24, 7j./7 ; 365j./an
700	sites - dont 75 % hors de l'Île-de-France – en métropole, en outre-mer et dans 90 emprises diplomatiques françaises
100 %	de disponibilité du réseau «coeur» en 2024
8 000	utilisateurs des systèmes interministériels classifiés
230 000	utilisateurs des téléphones mobiles sécurisés par l'OSIIC
6	plate-formes logistiques interministérielles

YVES VERHOEVEN

Directeur de l'Opérateur des systèmes d'information interministériels classifiés

> « L'OSIIC a assuré sa montée en puissance en cultivant une identité civilo-militaire »

Quel bilan dressez-vous de votre première année (et demie !) à la tête de l'OSIIC ?

Le chemin parcouru démontre la pertinence de la création de l'OSIIC. J'ai connu le centre de transmissions gouvernemental (CTG), j'ai connu la sous-direction numérique (SDN) de l'ANSSI et la fusion de ces deux entités était souhaitable. Aujourd'hui, nous avons atteint une masse critique et une fluidité dans notre travail quotidien qui sont à mettre au compte de la création de l'OSIIC.

Depuis sa création en 2020, l'OSIIC a assuré sa montée en puissance en cultivant une identité civilo-militaire originale, orientée vers l'innovation, l'audace, l'esprit d'équipe et le sens du service. Héritant une situation technique et opérationnelle hétérogène et complexe, l'OSIIC dispose aujourd'hui d'un bilan extrêmement satisfaisant : les systèmes d'information vieillissants ont connu des modernisations majeures, le service aux très hautes autorités a été assuré sans faille, les outils interministériels classifiés ont été largement déployés et sont désormais des outils indispensables, tant en administration centrale qu'en préfecture ou dans nos représentations diplomatiques à l'étranger.

C'est avec la conscience aiguë d'œuvrer pour la compétitivité de la France qu'une nouvelle feuille de route stratégique a été conçue collectivement. Elle offrira à l'OSIIC un cadre d'action ambitieux pour la période 2024-2027, qui nous guidera et nous fédérera, dans cet état d'esprit qui nous caractérise : le dépassement au service de grandes missions !

Quels défis majeurs l'OSIIC a-t-il rencontrés en 2024, et comment ces défis ont-ils été surmontés ?

En regardant dans le rétroviseur, 2024 est une excellente année avec de très bons résultats ! Nous avons traversé l'épreuve des jeux Olympiques et Paralympiques sans incident, tout en fournissant les moyens de communication attendus. Nous avons également accompagné les trois changements de Gouvernement. Par ailleurs, nous avons réalisé des progrès significatifs dans la transformation de nos systèmes d'information et nous avons enrichi de manière importante les outils collaboratifs sur ISIS et l'accès aux outils classifiés, *via* les *hubs* interministériels. Nous avons notablement accru la fourniture de services numériques spécialisés aux directions du SGDSN, à l'image du succès de la livraison de l'outil numérique d'aide à la gestion de crise ATHENA à nos collègues de la direction de la protection et de la sécurité de l'État. Enfin, nos efforts ont été récompensés par une augmentation significative du taux de satisfaction du service et de l'assistance aux utilisateurs du SGDSN.

En outre, 2024 a été une réussite concernant nos ressources humaines, avec un effectif total jamais atteint jusqu'ici. Sans répondre à tous nos besoins, cette croissance nous permet d'alimenter une ambition forte ; ce qui est une nécessité face à la menace et à l'exigence naturelle de nos utilisateurs. Enfin, 2024 nous a permis de finaliser notre cadre stratégique. Ce fut une année durant laquelle nous avons été portés par l'enthousiasme des travaux qui nous sont confiés et que nous nous attachons à réaliser dans un contexte budgétaire contraint.

Quels sont les grands enjeux à venir pour l'OSIIC ?

L'année 2025 sera l'occasion de mettre notre souplesse au défi, dans un contexte budgétaire incertain, tant en matière de fonctionnement, d'investissement que d'évolution de nos effectifs. Nous allons devoir adapter nos ambitions et notre programme de travail tout en nous montrant astucieux pour faire le plus possible avec un peu moins de moyens.

05

UN PAYSAGE INFORMATIONNEL COMPLEXE

2024, UNE ANNÉE D'ENGAGEMENT MAJEUR POUR VIGINUM DANS LA LUTTE CONTRE LES INGÉRENCES NUMÉRIQUES ÉTRANGÈRES

Moment charnière dans l'histoire récente de VIGINUM, l'année 2024 a été cadencée par l'organisation de plusieurs évènements majeurs qui auront marqué la vie publique nationale. Conformément aux termes de son décret de création et à sa vocation initiale, VIGINUM a directement participé à la protection du débat public numérique national lors de l'élection européenne et des élections législatives, en assurant une vigilance renforcée pour prévenir les tentatives de déstabilisation en ligne d'origine étrangère. De surcroît, le service s'est attaché à sensibiliser l'ensemble des parties prenantes aux élections, notamment les équipes de campagne ainsi que les autorités garantes.

En outre, dans le cadre de sa mission de protection des intérêts fondamentaux de la Nation (IFN), VIGINUM a contribué à la sécurisation des jeux Olympiques et Paralympiques de Paris 2024 en déployant un dispositif exceptionnel de détection, en étroite coordination avec les organisateurs, les partenaires interministériels du COLMI, ainsi que les médias et *fact-checkers*. Les 43 opérations détectées ont été décrites au sein d'un rapport public de synthèse sur la menace informationnelle observée durant l'évènement.

De plus, en coordination avec le ministère de l'Europe et des Affaires étrangères, VIGINUM a poursuivi la dénonciation publique des manœuvres informationnelles de nos compétiteurs, dans un contexte marqué par le durcissement des crises internationales, afin de sensibiliser l'opinion publique aux menaces liées aux manipulations de l'information. Le service a ainsi publié plusieurs rapports portant sur les manœuvres des réseaux russes de propagande *Portal Kombat* et *Matriochka* ainsi que sur les tentatives de déstabilisation opérées par l'Azerbaïdjan dans nos territoires ultra-marins, notamment au travers du *Baku Initiative Group*.

Parallèlement à ce fort engagement opérationnel, VIGINUM s'est attelé à développer une approche éducative à destination du grand public afin d'assurer une forme d'immunité durable de la société contre les manipulations de l'information. Cette démarche de sensibilisation de l'opinion publique passe également par un meilleur soutien aux acteurs de la société civile travaillant sur les sujets de lutte contre les manipulations de l'information. C'est pourquoi, dans une logique d'outillage de ces acteurs, VIGINUM a régulièrement publié sur son compte *GitHub* les éléments techniques associés aux campagnes informationnelles exposées. Il y met aussi librement à disposition les différents outils développés par son Datal@b.

Enfin, VIGINUM a contribué activement aux travaux européens et multilatéraux en matière de lutte contre les manipulations de l'information à travers la mise en œuvre d'actions d'accompagnement et d'assistance à destination de partenaires internationaux tels que la Moldavie.

UNE ACTIVITÉ OPÉRATIONNELLE SOUTENUE FACE À UNE MENACE INFORMATIONNELLE EN EXPANSION

Dans un contexte de vives tensions internationales, l'année 2024 a été marquée par une augmentation significative du nombre de campagnes numériques de manipulation de l'information visant les démocraties, notamment la France. Cette augmentation peut être corrélée au nombre élevé d'échéances électorales qui ont rythmé une année durant laquelle près de la moitié de la population mondiale en âge de voter a été appelée aux urnes.

Ainsi, VIGINUM a observé une profonde mutation des opérations d'ingérence numériques étrangères qui cherchent à instrumentaliser les tensions au sein des sociétés visées, pour *in fine* polariser l'opinion publique. Par ailleurs, ces manœuvres informationnelles se déploient sur des plateformes où elles peuvent être amplifiées du fait de la faiblesse de la modération et le développement de nouveaux vecteurs technologiques. Les acteurs de la menace informationnelle y font usage de procédés novateurs et très diversifiés comme l'usurpation d'identité visuelle (*typosquatting*), le ciblage des *fact-checkers* à des fins de déstabilisation, la création de fausses vidéos ou de faux contenus par des intelligences artificielles… afin de porter atteinte à la confiance de la population envers les institutions et les médias, et de cibler ainsi le cœur de notre système démocratique.

RAPPORTS PUBLIÉS

FÉVRIER 2024

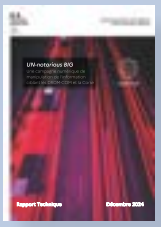
Portal Kombat : un réseau structuré et coordonné de propagande prorusse. Entre les mois de septembre et décembre 2023, VIGINUM a analysé l'activité d'un réseau de 193 portails d'information aux caractéristiques similaires et diffusant des contenus pro-russes à destination de publics internationaux, dont français.

AVRIL 2024

Portal Kombat : extension du réseau de propagande russe. Avec désormais 224 « portails d'information » numérique identifiés comme appartenant au réseau Portal Kombat, VIGINUM a détecté un « quadrillage informationnel » méticuleux de ce réseau, ciblant l'audience de presque tous les États membres de l'UE.

JUIN 2024

Matriochka : une campagne prorusse ciblant les médias et la communauté des fact-checkers. Ce mode opératoire, actif depuis septembre 2023, s'appuie sur la publication de faux contenus qui font ensuite l'objet d'une diffusion coordonnée dans l'espace réponse des publications de comptes X de médias et de cellules de *fact-checking* de plus d'une soixantaine de pays. Les faux contenus diffusés usurpent généralement l'identité de personnalités et de médias nord-américains ou européens, y compris français. S'ils propagent et amplifient majoritairement des narratifs anti-ukrainiens, ces contenus prennent également pour cible la politique française de soutien à l'Ukraine, certaines personnalités politiques françaises ainsi que les jeux Olympiques et Paralympiques de Paris 2024 afin de décrédibiliser les médias et personnalités ciblés tout en promouvant des contenus servant les intérêts russes.



DÉCEMBRE 2024

UN-notorious BIG : une campagne numérique de manipulation de l'information ciblant les DROM-COM et la Corse. Dans ce rapport, VIGINUM a analysé l'activité numérique d'une organisation, étroitement liée au pouvoir azerbaidjanais, nommée *Baku Initiative Group* (BIG), et diffusant des contenus à la ligne éditoriale résolument hostile à la France. L'écosystème lié au BIG cherche délibérément à exploiter la situation politique et économique dans les départements, régions et collectivités d'Outre-Mer (DROM-COM) et en Corse ainsi qu'à instrumentaliser l'histoire de la présence française sur le continent africain à des fins malveillantes.

FÉVRIER 2024

Portal Kombat : suite des investigations sur le réseau structuré et coordonné de propagande prorusse. VIGINUM caractérise l'implication d'une entreprise russe domiciliée en Crimée, « Tigerweb », dans la création et l'administration des sites du réseau Portal Kombat.

MAI 2024

Nouvelle-Calédonie : manœuvre informationnelle impliquant des acteurs azerbaïdjanais. Dans le contexte des émeutes du mois de mai 2024 en Nouvelle-Calédonie, VIGINUM a détecté plusieurs manœuvres informationnelles visant la France et impliquant des acteurs azerbaïdjanais. Le service a en effet détecté sur différentes plateformes, la propagation massive et coordonnée de contenus manifestement inexacts ou trompeurs accusant la police française de tirer sur des manifestants indépendantistes.

SEPTEMBRE 2024

Synthèse de la menace informationnelle ayant visé les jeux Olympiques et Paralympiques de Paris 2024. VIGINUM a identifié 43 manœuvres informationnelles ayant ciblé les jeux de Paris 2024, s'appuyant sur différents modes opératoires documentés. Si celles-ci se révèlent majoritairement opportunistes, le service a également caractérisé deux campagnes numériques planifiées et coordonnées de manipulation de l'information, dont une à l'été 2023, désignée sous le nom « *OLIMPIYA* », et impliquant des acteurs pro-azerbaïdjanais.

UN COLLECTIF DE TRAVAIL ET UNE ÉQUIPE PLURIDISCIPLINAIRE POUR TRAITER LES ÉVOLUTIONS DE LA MENACE INFORMATIONNELLE

Afin de rester à l'état de l'art sur les défis posés par la menace informationnelle, VIGINUM a fait évoluer sa structure interne, consolidée par de nouveaux recrutements. Pour ce faire, le service s'est notamment doté d'une cellule d'anticipation qui lui offre une capacité à suivre l'évolution technique des plateformes.

En parallèle, VIGINUM a poursuivi sa dynamique de croissance des effectifs avec 24 recrutements en 2024, comprenant aussi bien des spécialistes issus des sciences politiques que des ingénieurs. Le pôle technique a ainsi été renforcé, notamment pour permettre le développement d'outils de détection destinés à être mis à la disposition de la communauté des acteurs de la lutte contre les manipulations de l'information.

90 %	de cadres dont 54 % de femmes et 46 % d'hommes
56	agents au 31 décembre 2024
33	ans d'âge moyen

FOCUS SUR D3LTA

Développé par le Datal@b de VIGINUM, le code Python de l'outil D3LTA a été publié en ligne en 2024. Il permet de détecter, sur les plateformes, le contenu dupliqué de manière inauthentique par le biais de reformulations ou de traductions, échappant ainsi au processus de modération. Outil opérationnel utilisé par les équipes de VIGINUM dans le cadre de leur mission de détection et de caractérisation des manœuvres d'ingérences numériques étrangères ce code est désormais à la disposition des acteurs de la société civile qui ont tout loisir de l'utiliser et de l'améliorer, de façon collaborative.

UNE COORDINATION ET UNE COLLABORATION RENFORCÉE POUR LUTTER CONTRE LES MANIPULATIONS DE L'INFORMATION

Au cœur du dispositif national de lutte contre les manipulations de l'information, VIGINUM participe au Comité opérationnel de lutte contre les manipulations de l'information (COLMI) et assiste le SGDSN dans sa mission d'animation et de coordination des travaux interministériels portant sur protection de la population contre les ingérences numériques étrangères.

Dans ce cadre, VIGINUM a directement contribué aux actions de communication stratégique du ministère de l'Europe et des Affaires étrangères en exposant quatre manœuvres informationnelles à travers la publication de rapports techniques. De surcroît, certaines de ces manœuvres ont fait l'objet d'une dénonciation publique.

En tant que chef de file de l'action de l'État en matière de lutte contre les manipulations de l'information, VIGINUM a mis à profit l'année 2024 pour mener ses premières actions de sensibilisation, d'éducation et d'information à destination du grand public. Une priorité a été accordée aux jeunes publics en s'attachant à mettre à leur disposition des ressources pédagogiques s'inscrivant dans les programmes d'éducation aux médias. VIGINUM a également animé plusieurs sessions de sensibilisation à la menace informationnelle au profit d'acteurs du monde économiques français. En outre, VIGINUM a renforcé ses liens avec le monde académique en contribuant à la recherche dans le domaine de la LMI au travers du financement d'études et de programmes de recherches, mais aussi par la publication de quatre articles académiques et la mise à disposition en source ouverte de trois codes d'outils.

SIGNATURE CONVENTION ARCOM

Après la signature en décembre 2023 d'une convention avec Pharos, VIGINUM a franchi une nouvelle étape en juillet 2024 avec la signature d'une convention avec l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom). Cette convention précise les modalités de coopération entre les deux entités, en particulier dans l'application du règlement européen sur les services numériques (DSA). La convention, signée en amont des jeux Olympiques et Paralympiques de Paris 2024 vise également à intensifier les échanges et la mise en commun des expertises pour lutter plus efficacement contre les tentatives d'ingérences numériques étrangères.

ANNE-SOPHIE **DHIVER**

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

« Le service a significativement accéléré son ouverture aux partenaires internationaux. »

Quelles appréciations faites-vous de l'état de la menace en 2024 ?

L'année 2024 a été malheureusement marquée par un durcissement de la menace informationnelle, dans un contexte de pressions accrues sur la sphère de l'information numérique. Pression stratégique d'abord, car cette année encore, nos écosystèmes informationnels ont été le théâtre de rivalités internationales désinhibées, où des acteurs étrangers tentent de manipuler le débat public numérique afin de déstabiliser le fonctionnement des sociétés démocratiques. Pression systémique ensuite, du fait de la compétition que se livrent de grandes entreprises technologiques pour la domination de la sphère de l'information numérique, avec, au cœur de cette lutte, l'intelligence artificielle (IA). L'essor de l'IA générative est ainsi venu cette année amplifier encore les menaces qui pèsent sur nos écosystèmes informationnels.

Quels effets sur la France ?

S'agissant spécifiquement de la menace informationnelle ayant visé les intérêts français, il me semble que nous pouvons dégager trois tendances principales. Tout d'abord, 2024 a confirmé que les conflits en cours offraient un terrain extrêmement attractif pour la menace informationnelle, et ce bien au-delà des seuls belligérants impliqués. C'est ce que nous avons pu mettre à jour notamment au travers de plusieurs rapports publics, tels que *Portal Kombat* et *Matriochka*, deux opérations pro-russes visant des auditoires internationaux.

Ensuite, cette année a également confirmé que les grands évènements tels les scrutins nationaux ou les évènements sportifs d'envergure mondiale, de par leur résonance médiatique, sont un théâtre d'opération privilégié pour les acteurs de la menace informationnelle. VIGINUM a ainsi détecté 43 manœuvres informationnelles ayant visé les jeux Olympiques et Paralympiques de Paris.

Enfin, la menace informationnelle a particulièrement ciblé les intérêts français dans nos départements et collectivités d'outre-mer. Nous avons ainsi mis au jour, au travers d'une fiche technique et de notre rapport public *UN-notorious BIG*, comment des acteurs pro-azerbaïdjanais tentent notamment d'exploiter la situation en Nouvelle-Calédonie et visent de façon répétée de nombreux DROM-COM et la Corse.

VIGINUM est un modèle unique au monde, comment travaillez-vous avec les autres pays ?

En 2024, le service a significativement accéléré son ouverture aux partenaires internationaux, avec un double objectif : d'une part, exporter l'approche et l'expertise françaises de lutte contre les manipulations de l'information ; d'autre part, renforcer notre capacité à agir collectivement face à une menace persistante, qui met aujourd'hui à l'épreuve l'ensemble des démocraties, notamment européennes. C'est ce que nous avons fait avec le ministère de l'Europe et des affaires étrangères en dénonçant publiquement les agissements des acteurs pro-russes dans le cadre du format Weimar, avec nos partenaires allemands et polonais.

A cette fin, notre stratégie internationale s'est principalement déclinée en trois axes : des coopérations bilatérales afin d'échanger sur des aspects opérationnels choisis ; un accompagnement notamment technique pour des partenaires affinitaires ; notre participation aux travaux de plusieurs instances multilatérales en matière de lutte contre les manipulations de l'information. L'ensemble de ces coopérations n'a qu'un seul objectif : renforcer la capacité de la France, et plus largement de l'ensemble des démocraties, à répondre aux menaces hybrides dans le champ informationnel.

JEAN-LUC SAURON

Conseiller d'État,
Président du comité éthique et scientifique

« Garantir le droit et conseiller

Quel est le rôle du comité éthique et scientifique ?

Magistrat, diplomate, journalistes, chercheur en sciences, expert en numérique, régulateur des médias, spécialiste du droit, le comité éthique et scientifique regroupe huit personnalités aux profils très différents. Garantir le droit et conseiller, le comité a deux grandes missions : il veille à ce que l'activité du service soit conforme au cadre réglementaire en vigueur, notamment lors de la mise en œuvre du traitement des données à caractère personnel prévu dans le décret n° 2021-1587 du 7 décembre 2021 ; il a aussi un rôle plus prospectif, à la fois d'évaluation du cadre réglementaire et de réflexion sur des questions plus techniques, scientifiques ou sociétales parmi lesquelles l'identification des enjeux éthiques des travaux menés par les agents de VIGINUM. Le comité parvient ainsi à traiter un large éventail de sujets grâce à l'accès total à l'ensemble des travaux du service – nous y avons veillé en bonne intelligence avec son chef, Marc-Antoine Brillant,– et aux compétences de ses membres qui couvrent de nombreux domaines d'expertise.

Quels ont été les aspects les plus marquants de votre travail en 2024 ?

L'année 2024 a été ma première année de présidence du comité. Elle a été marquée par deux séries d'évènements : les jeux Olympiques et Paralympiques qui étaient identifiés comme un moment important en raison de la résonance médiatique qu'ils offraient, d'une part ; les élections européenne et législatives, d'autre part. Ces évènements ont tout particulièrement retenu notre attention, notamment les élections : en effet le comité, en liaison avec l'Arcom et les autres autorités publiques impliquées dans les processus électoraux, peut être amené à recommander certaines mesures à VIGINUM en cas de questionnement ou de problème.

Indépendamment de ces évènements, nous nous sommes mobilisés sur plusieurs chantiers d'évolution à court terme des activités de VIGINUM comme l'évolution de son cadre juridique, le développement de sa mission de sensibilisation de la société française aux menaces informationnelles, les réflexions sur les questionnements éthiques concernant son activité et celle de ses agents mais aussi sur des questions plus prospectives, comme les effets de l'intelligence artificielle – positifs ou négatifs – en matière d'ingérences numériques.

Quelle appréciation d'ensemble portez-vous sur la question des ingérences numériques étrangères ?

Il convient de relever la très nette accélération de ce phénomène. S'il est possible de considérer la campagne du *Brexit* comme la première manifestation d'ampleur des ingérences numériques étrangères, en 2016, immédiatement suivie par la tentative dite des *Macronleaks* dans la campagne présidentielle de 2017, l'invasion de l'Ukraine marque un tournant matérialisé par une quasi quotidienneté de ce type d'activités hostiles aux intérêts de la Nation. L'année 2024 a connu (en dehors des JOP et des élections nationale et européenne précitées) trois ingérences majeures dans des campagnes électorales en Géorgie, en Moldavie et en Roumanie. La dernière, qui a conduit à l'annulation de cette élection présidentielle pour ingérence étrangère, pour la première fois dans un pays démocratique me semble-t-il, doit nous interroger profondément. L'excellent rapport publié par VIGINUM sur les procédés techniques informationnels observés lors de ces élections souligne combien ces mêmes méthodes pourraient être utilisées à l'encontre de la France, altérant la sincérité du débat démocratique et par suite les résultats des élections. Certes les séries télévisées se font de plus en plus l'écho de ces manœuvres, mais notre opinion publique ne me paraît pas suffisamment consciente de cette menace.
VIGINUM est un service jeune. Ses responsables et agents font un travail remarquable reconnu partout au sein des pays démocratiques, y compris hors d'Europe. Dans un contexte où la France est amenée à prendre des positions fortes, où les menaces sur la qualité de notre vie démocratique pourraient s'accentuer, il paraît fondamental de lui donner encore plus de moyens juridiques, humains et technologiques, non pour rester à hauteur de la menace, mais, et le cas roumain l'a démontré, pour savoir l'anticiper et y répondre afin que nos concitoyens restent maîtres de leurs choix politiques et sociétaux. Le comité éthique et scientifique se mobilise.

06

ASSEOIR UNE VISION STRATÉGIQUE DU NUCLÉAIRE

ÉVOLUTIONS DU RÔLE ET DES MISSIONS DU HAUT-COMMISSAIRE À L'ÉNERGIE ATOMIQUE

Le haut-commissaire à l'Énergie atomique (HCEA) a vu ses missions très largement modifiées en 2024. Jusqu'en 2023, ces missions étaient de deux ordres :

- une mission originelle d'orientation des recherches menées par le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) qui fondait la répartition des rôles à la tête du commissariat entre un administrateur général chargé de l'organisation et de la direction de l'établissement et un haut-commissaire chargé de l'orientation des recherches ;
- une seconde mission d'expertise scientifique sur l'énergie nucléaire et ses applications, civiles et de défense, en appui au Gouvernement. Cette mission, importante au début de l'aventure nucléaire en France, s'est peu à peu étiolée jusqu'au périgée de la décennie 2010-2020.

En 2023, la décision a été prise de revenir sur cette organisation. Elle a été matérialisée par le décret n° 2023-1383 du 30 décembre 2023 relatif au conseil de politique nucléaire et au haut-commissaire à l'Énergie atomique qui a confié le secrétariat du conseil de politique nucléaire au secrétaire général de la défense et de la sécurité nationale et qui a rattaché le haut-commissaire à l'énergie atomique au SGDSN, pour sa gestion administrative et budgétaire.

Ce choix a notamment résulté de la volonté de l'État de reprendre en main les questions de politique nucléaire et d'en asseoir la vision stratégique sur des bases scientifiques et techniques. À cette fin, le haut-commissaire est donc désormais placé immédiatement sous le Premier ministre.

Cette nouvelle organisation est adaptée aux caractéristiques propres du domaine de l'énergie nucléaire, sujet éminemment stratégique et particulièrement technique. La mise en cohérence de l'ensemble des décisions est complexe, principalement en raison d'une cascade de conséquences. Ainsi, toute décision portant sur les réacteurs entraîne des effets sur le cycle associé, sur les déchets, sur l'outil industriel, *etc*. Cette complexité intrinsèque impose des délais d'instruction importants avant que des analyses et propositions de décisions puissent être soumises à la décision politique. De surcroît, elle impose un niveau de compétence technique élevé afin de délivrer des avis indépendants de la vision portée par les grands acteurs du domaine.

La mission principale du HCEA est donc « redevenue » d'assister l'État dans la relance d'un programme nucléaire ambitieux, dans l'élaboration de la stratégie nationale et la vérification de sa cohérence sur l'ensemble des composantes du « système » nucléaire. Par délégation du secrétaire général de la défense et de la sécurité nationale, le haut-commissaire prépare les conseils de politique nucléaire, en assure le secrétariat et opère le suivi de la mise en œuvre des décisions. De surcroît, le haut-commissaire est désormais tenu par la loi de remettre un rapport annuel sur l'état des activités nucléaires civiles, notamment de production et de recherche, et de rendre de multiples avis, en particulier sur la programmation pluriannuelle de l'énergie. Enfin, le HCEA émet des avis à la demande du Président de la République, du Premier ministre ou des ministres impliqués dans la politique nucléaire.

Par ailleurs, le haut-commissaire demeure président du conseil scientifique du CEA.

Le HCEA reste l'autorité de contrôle indépendante de la direction des applications militaires du CEA sur une partie de ses missions. Il est à la tête de la chaîne de sécurité pour les installations nucléaires intéressant la dissuasion ne relevant pas du ministère des armées et il est chargé de veiller, dans une vision de long terme, à la cohérence de l'ensemble des données recueillies au titre de la gestion patrimoniale des matières nucléaires nécessaires à la défense. Pour ce faire, il dispose de la direction déléguée au contrôle gouvernemental.

ACTIVITÉS DU HCEA EN 2024

Les activités du HCEA en 2024, hors sujets intéressant la défense, peuvent se résumer sommairement en huit points :

- la préparation des réunions du conseil de politique nucléaire (CPN) et le suivi des décisions prises, *via* des réunions avec les cabinets ministériels ou les administrations, et en liaison avec de nombreux acteurs industriels, privés et publics;

- une mission *ad hoc*, confiée par le CPN de février 2024 au haut-commissaire, d'évaluation des projets de réacteurs modulaires innovants dits *AMR* ou *SMR*. Cette mission s'est décomposée en trois grandes phases, la dernière étant toujours en cours :

  - une première phase de trois à quatre mois d'analyse préalable des douze projets, avec des rencontres multiples avec leurs auteurs ;

  - la rédaction d'un rapport d'ensemble sur les projets et les questions techniques traitées ou demeurant à traiter. Les conclusions de ce rapport ont vocation à être examinées par le conseil de politique nucléaire et l'audition des soumissionnaires ;

  - après les auditions, la restitution des conclusions aux différents auteurs et le suivi continu de l'évolution des douze projets.

- diverses productions stratégiques sur l'avenir de la filière nucléaire et la fermeture du cycle du combustible ;

- des expertises ponctuelles sur des sujets traités en CPN ou non notamment dans les activités de défense ;

- la présidence du Conseil scientifique du CEA – un Conseil scientifique sur la diffusion neutronique en juin 2024 et un Conseil scientifique en novembre 2024 sur le suivi des recommandations sur le numérique et sur l'activité de recherche & développement dans le domaine nucléaire ;

- une activité soutenue en direction des parlementaires, de la communauté scientifique nationale, de la société française d'énergie nucléaire, et de la Cour des Comptes ;

- une analyse de la politique pluriannuelle de l'énergie en vue de l'émission d'un avis, tel que prévu par l'article L. 141-13 du code de l'énergie ;

- la présidence de l'Institut International de l'Énergie Nucléaire (I2EN), qui a pour mission de fournir aux pays étrangers des solutions de formation pour subvenir à leurs besoins en personnel qualifié. Ainsi, l'I2EN assiste et guide ces pays dans le développement de leurs propres systèmes éducatifs nucléaires.

PERSPECTIVES 2025

Outre la poursuite des activités régaliennes largement synthétisées lors des conseils de politique nucléaire et les activités scientifiques découlant de la présidence du conseil scientifique du CEA et de l'I2EN, l'année 2025 sera marquée par le traitement de deux sujets d'importance, engagé en 2024 :

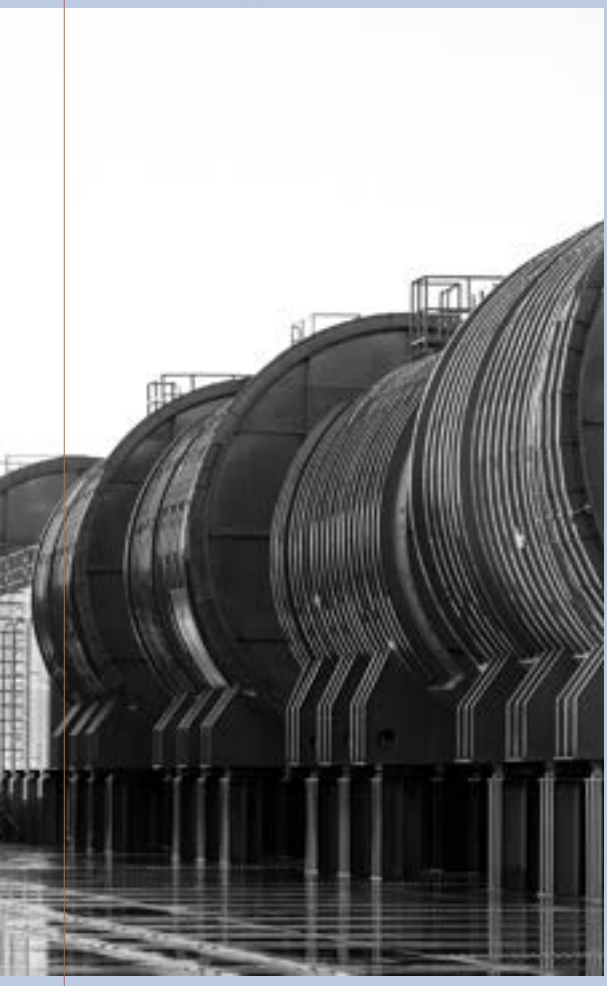
- la préparation de la fermeture du cycle, avec des travaux plus poussés sur le cycle du combustible, sur les choix technologiques en matière de petits réacteurs et sur l'organisation industrielle à mettre en œuvre pour donner les meilleures chances de succès à l'émergence d'un prototype ;

- le suivi et l'accompagnement des projets de réacteurs *AMR-SMR*, sous une forme à préciser, dans la phase 2 du plan d'investissement France 2030. La compétence acquise dans l'évaluation de ce type de nouveaux réacteurs pourra être utilisée dans de nouveaux domaines.

- de surcroît, un troisième sujet d'ampleur sera probablement traité : la simplification de certaines contraintes applicables au nucléaire. Tant les grands industriels de la filière nucléaire que les porteurs de projets de nouveaux réacteurs se sont engagés dans des démarches de réforme des processus de prise de décision, de simplification des concepts industriels, des organisations, mais aussi des grands documents de sûreté, *etc.* Le HCEA contribuera à proposer des solutions de simplifications acceptables sans renoncement aux nécessités de sûreté et de sécurité.

Le HCEA devra aussi émettre un avis général sur les activités nucléaires civiles, conformément à l'article L. 141-13 du code de l'énergie et sur la programmation de la politique énergétique.

LE CONSEIL DE POLITIQUE NUCLÉAIRE



Présidé par le Président de la République, le conseil de politique nucléaire définit les grandes orientations de la politique nucléaire et veille à leur mise en œuvre, notamment en matière d'exportation et de coopération internationale ; de politique industrielle ; de politique énergétique ; de recherche ; de sûreté ; de sécurité et de protection de l'environnement.

Convoqué par le Président de la République, le Conseil de politique nucléaire réunit le Premier ministre, les ministres en charge de l'énergie ; de l'Europe et des affaires étrangères ; du commerce extérieur ; de l'économie ; du budget ; de l'industrie ; de la recherche et de la défense, ainsi que le chef d'état-major des armées ; le secrétaire général de la défense et de la sécurité nationale et l'administrateur général du Commissariat à l'énergie atomique.

En fonction de l'ordre du jour, d'autres membres du Gouvernement peuvent être ponctuellement invités, ainsi que le président de l'Autorité de sûreté nucléaire et de radioprotection, des hauts fonctionnaires civils et militaires ou encore le Haut-commissaire à l'énergie atomique.

Au titre de son rôle de secrétaire du Conseil de politique nucléaire, le SGDSN coordonne les travaux de préparation, assure le suivi des orientations et des décisions prises et apporte son expertise en matière de politique nucléaire au niveau interministériel. Pour ce faire, le SGDSN peut s'appuyer sur le Haut-commissaire à l'énergie atomique qui lui est rattaché par le décret n° 2023-1383 du 30 décembre 2023.

En 2024, le CPN a réaffirmé les orientations nationales sur l'aval du cycle du combustible nucléaire, à savoir le retraitement, la réutilisation des combustibles usagés et la fermeture du cycle. La réunion du CPN fut ainsi l'occasion d'annoncer que des investissements importants seraient consentis pour le site de retraitement des déchets d'Orano, à La Hague.

VINCENT **BERGER**

Haut-commissaire à l'Énergie atomique

> DEPUIS LA RELANCE DU NUCLÉAIRE VOULUE PAR LE PRÉSIDENT DE LA RÉPUBLIQUE LORS DU DISCOURS DE BELFORT, LES ACTEURS S'ALIGNENT POUR CONSTRUIRE UNE POLITIQUE NUCLÉAIRE AMBITIEUSE.

Physicien, il a été président de l'université Paris-Diderot de 2009 à 2013. Conseiller du Président de la République pour les questions d'éducation, d'enseignement et de recherche de 2013 à 2015, il est ensuite directeur de la recherche fondamentale du CEA de 2015 à 2019. Nommé conseiller-maître à la Cour des comptes en 2020, il a été nommé haut-commissaire à l'énergie atomique (HCEA) en septembre 2023. Depuis le 1er janvier 2024, le HCEA est rattaché au Secrétaire général de la défense et de la sécurité nationale pour sa gestion administrative et budgétaire.

07

SOUTENIR LE RENSEIGNEMENT

UNE MOBILISATION OLYMPIQUE

Vu du grand public, il y a bien eu une trêve olympique : les jeux se sont déroulés sans heurts. Vu des agents de l'ombre, de la sécurité et du renseignement, l'année 2024 fut – dès la fin 2023 – une année de mobilisation inédite. Pour le GIC, la période fut extrêmement exigeante, marquée par une présence accrue, des horaires étendus, des brigades et des permanences renforcées. Un contrat opérationnel élaboré à tous les niveaux hiérarchiques du GIC a été établi fin 2023 et respecté en 2024 par tous les agents, résolument tournés vers le même objectif : se placer « au service des services » et offrir au Premier ministre une vision synoptique, en temps réel, des surveillances autorisées.

Des mois avant l'arrivée de la flamme, le GIC s'est aussi préparé techniquement pour éviter « le coup de la panne » pendant les jeux et s'assurer que ses systèmes d'information tiendraient la cadence. Les migrations techniques ont été accélérées pour armer les fonctions critiques avec des matériels neufs. Le GIC a également accéléré le déménagement des services parisiens d'exploitation vers son nouveau bâtiment. Les services particulièrement concernés par les jeux étaient pleinement opérationnels dans leurs nouveaux bureaux dès le mois de mars. Les suivants les ont rejoints juste après les jeux.

Malgré la forte pression sécuritaire et le pic d'activité à la fin du printemps et à l'été, le dispositif des techniques de renseignement ne s'est jamais écarté des limites de la loi et l'équilibre entre les exigences de sécurité nationale et le droit au respect de la vie privée a été préservé. La progression du nombre d'autorisations de techniques de renseignement de 2023 à 2024 a été de 3 %. Ce pourcentage doit cependant être interprété car la comptabilisation de la technique, très utilisée, de géolocalisation en temps réel régie par l'article L. 851-4 du code de la sécurité intérieure a changé fin 2023 : avant cette date, elle était comptabilisée par identifiant ; depuis, le décompte se fait par personne surveillée, or une personne peut utiliser, simultanément ou successivement, plusieurs identifiants. Dans le même temps, le nombre d'interceptions de sécurité a augmenté de 10 %. Il dépasse celui, cumulé, des captations de paroles, d'images, de données informatiques et d'introductions dans les lieux privés. Ainsi, une nouvelle fois, la technique historique des « écoutes » s'impose comme un outil indispensable pour les services, même si elle n'est plus celle par laquelle ils apprennent la teneur détaillée de projets terroristes, d'ingérence, d'espionnage, de criminalité organisée ou de violences collectives.

CHIFFRES

1 174	agents des services formés par le GIC
~100 000	autorisations de techniques de renseignement
1 250	transcriptions contrôlées chaque jour
21	nouveaux opérateurs interlocuteurs du GIC

LA DÉTECTION ALGORITHMIQUE DES MENACES

Le GIC a développé et mis en œuvre de nouveaux algorithmes au profit de certains services pour la prévention du terrorisme. Il a largement contribué au rapport remis au Parlement sur les algorithmes fin juillet 2024. Il a entamé un travail de recension des besoins auprès des services du premier cercle pour élaborer des algorithmes innovants ayant pour objet la contre-ingérence et la cyberdéfense, domaines ouverts aux algorithmes depuis la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France.

DES TRAVAUX INTERMINISTÉRIELS

Le recueil de données informatiques, technique conçue par le législateur en 2015 pour permettre, lorsque l'interception ne suffit pas, l'accès aux données en clair de la personne visée, peut s'exercer depuis 2021 avec le concours des opérateurs. Elle s'installe dans le paysage des techniques de renseignement. La Commission nationale de contrôle des techniques de renseignement a souhaité que des garanties renforcées s'appliquent aux recueils de données informatiques et le Gouvernement a répondu favorablement à cette demande. Un travail préparatoire important a été effectué pour qu'un programme interministériel conduit par le GIC, avec la direction générale de la sécurité intérieure et la direction générale de la sécurité extérieure, puisse être lancé à la fin de la période olympique. Ce programme est structurant pour le GIC dans les années à venir. Il permettra d'offrir à la Commission nationale de contrôle des techniques de renseignement le regard nécessaire à son contrôle et aux services des moyens d'exploitation plus performants, non seulement des données informatiques recueillies mais aussi des communications interceptées.

Les 300 agents du GIC, répartis sur le site historique, le nouveau bâtiment et quelques centres en province, ont prouvé en 2024 leur dévouement et leur engagement. Pour 2025 et au-delà, leurs priorités sont clairement définies :

- donner toute leur portée opérationnelle aux algorithmes en vigueur, poursuivre la fluidification du traitement des détections, répondre aux besoins exprimés par les services pour concevoir, développer, compiler et exécuter des algorithmes pour la poursuite d'autres finalités que la prévention du terrorisme dans le nouveau champ ouvert par la loi du 25 juillet 2024 ;

- conduire le programme interministériel de centralisation des recueils de données informatiques, d'abord au profit de la direction générale de la sécurité intérieure et de la direction générale de la sécurité extérieure, et poursuivre ses initiatives en la matière au profit des autres services.

Le Premier ministre est tête de chaîne du renseignement (article 21 de la Constitution) et c'est sous son autorité que sont diligentées et mises en œuvre les techniques de renseignement. Si l'année 2024 a connu quatre Premiers ministres, les techniques de renseignement n'ont souffert d'aucune interruption, même d'une journée. Les processus qui les entourent sont éprouvés et leur continuité est assurée.

Depuis bientôt dix ans, le GIC accomplit ses missions dans un cadre légal posé en 2015 qui n'a jamais dévié de ses principes fondateurs malgré un rythme soutenu de modifications. La proposition de loi visant à sortir la France du piège du narcotrafic marquera vraisemblablement une nouvelle étape, confortant la position centrale du GIC, au cœur du renseignement.

CAPTEUR DE RENSEIGNEMENT

Les opérateurs de communications électroniques et autres fournisseurs de services de communication sur Internet constituent un capteur majeur de renseignement. C'est à eux que le GIC adresse quotidiennement des « ordres », comme le prévoit l'article L. 871-6 du code de la sécurité intérieure, visant à recueillir des données, entreposées ou transportées. Pour contribuer à la sécurité des jeux, la coopération des opérateurs a été remarquable. Ils se sont organisés et leurs équipes se sont mobilisées pour répondre, parfois dans des délais très brefs, aux réquisitions du GIC. La croissance du nombre de réquisitions, en direction des opérateurs comme acteurs dits *over the top*, a été extrêmement marquée, et le GIC a établi des liens opérationnels avec 21 nouveaux acteurs du numérique.

Les services ont corrélativement effectué plus de transcriptions et sollicité plus d'extractions, notamment sur les renseignements centralisés au GIC et soumis à son contrôle, préalablement à leur capitalisation au sein des services. Le GIC s'est organisé, en liaison avec les services, pour absorber les pics de charge qui ont correspondu à certains évènements publics liés aux jeux au cours desquels des menaces particulières avaient été identifiées.

Au profit des services, le GIC a intensifié ses actions de formation, notamment auprès des exploitants affectés en renfort pour les jeux, afin que ceux-ci s'approprient les outils informatiques du groupement interministériel de contrôle. Pour être au plus près des enquêteurs, le GIC a ouvert un nouveau centre d'exploitation dans une grande ville de l'Ouest de la France ; accueilli la direction du renseignement et de la sécurité de la défense dans deux centres en province et la direction nationale de la police judiciaire dans deux autres, y compris outre-mer ; étendu un centre dans le sud-ouest ; et contribué à la mise en place d'un nouveau centre technique en province.

Le GIC, aux côtés de la direction générale de la sécurité intérieure, a œuvré pour donner corps à la technique dite d'interception de sécurité satellitaire, afin que le Gouvernement puisse rendre compte au Parlement de l'expérimentation de la technique prévue à l'article L. 852-3 conformément aux dispositions de la loi du 30 juillet 2021.

08

UN SOUTIEN ACTIF

Le service de l'administration générale (SAG), service à vocation transversale, anime et coordonne l'ensemble des missions d'administration générale nécessaires à l'activité du SGDSN, ainsi qu'à celle du groupement interministériel de contrôle. Le service emploie une centaine d'agents de statuts divers, répartis entre deux sous-directions : celle en charge des ressources humaines et celle en charge de l'administration générale et des finances, auxquelles s'ajoute le détachement de gendarmerie en charge de la protection des sites.

L'année 2024 a été marquée, comme pour l'ensemble du SGDSN, par les jeux Olympiques et Paralympiques de Paris, en soutien actif aux directions en charge de la sécurisation de cet évènement. La préparation des JOP a été l'occasion d'accélérer et mettre en œuvre un ensemble d'opérations en cours, dans le domaine de la gestion des ressources humaines, de la logistique, du casernement… Ainsi, le régime des diverses astreintes a été mis à jour, la Tour Mercure a de nouveau été largement réaménagée, des opérations de fiabilisation des réseaux techniques ont été menées. Afin de faire face à d'éventuelles difficultés de transport en commun, des vélos électriques ont été mis à la disposition des agents. Enfin, le paiement des indemnités d'activité exceptionnelles, réservées au personnel particulièrement mobilisé pendant les JOP a été effectué, dans un contexte budgétaire complexe.

LES RESSOURCES HUMAINES

Dans le cadre de la transformation numérique du SGDSN, un effort particulier a été fait sur la mise en œuvre du module de paie du système d'informations RenoiRH. Ce système permet désormais de gérer tous les actes administratifs avec le même outil et assure la paie des agents. Sous des aspects techniques, cette modernisation est un pas important vers la dématérialisation des processus de ressources humaines.

Les annulations de crédits intervenues au mois de février ont amené le SAG à renforcer le pilotage des crédits de masse salariale et à mettre en œuvre de mesures d'économies, sans pour autant dégrader l'activité des directions. Ces mesures ont permis au SGDSN de poursuivre ses recrutements tout au long de l'année, de réaliser son schéma d'emploi et de préserver l'ensemble de ses emplois.

Le bureau de gestion du personnel militaire a achevé la rénovation du référentiel en organisation des postes militaires du SGDSN. Il a mené à bien les travaux préparatoires permettant le versement en 2025 de la prime de compétence spécifique du numérique, destinée aux militaires du SGDSN qui participent directement à la supériorité des forces armées dans l'espace numérique.

L'entrée en vigueur au 1er janvier 2025 de la protection sociale complémentaire, notamment du volet santé, désormais obligatoire, a nécessité une série d'actions spécifiques. La sous-direction des finances a notamment contribué à l'analyse des offres des soumissionnaires, menée par la direction des services administratifs et financiers du Premier ministre. Une fois le prestataire choisi, le SAG a décliné le plan ministériel de communication en direction des agents. Parallèlement, une opération a également été menée, durant l'automne, pour informer les agents de l'offre retenue pour assurer le volet prévoyance. Dès la paie du mois de janvier 2025, la sous-direction des ressources humaines a assuré le versement des contributions de l'État à tous les agents nouvellement affiliés. Désormais, les futurs agents sont informés des démarches à effectuer et la participation financière de l'État leur est versée dès le mois de leur arrivée.

En 2024, un plan d'action a été mis en œuvre pour parfaire l'information des agents sur les pathologies reconnues en tant que handicap, ainsi que sur les modalités de reconnaissance de la qualité de travailleur handicapé et les droits y afférents. De plus, des opérations de sensibilisation au handicap, menées à destination de l'ensemble des agents, ont été organisées, notamment au travers des partenariats avec l'association Accompagner la réalisation des projets d'études de jeunes élèves et étudiants handicapés (Arpejeh) et le Cercle sportif de l'institution nationale des Invalides (CSINI).

Parallèlement, le SGDSN a engagé, avec Pascal Chiron, délégué à l'encadrement supérieur des services du Premier ministre, un travail de fond pour mieux accompagner ses cadres supérieurs, notamment en termes de formation sur ces questions.

375 arrivées

304 départs

Dans le cadre de la Semaine européenne pour l'emploi des personnes handicapées, un séminaire « Le handicap, une diversité, une opportunité pour le collectif de travail » a été organisé le 19 novembre 2024. Il a réuni 80 agents. De surcroît, le SGDSN a renouvelé sa participation au DuoDay pour la 3ème année consécutive. Au total, en 2024, 22 agents ont transmis et/ou ont obtenu leur reconnaissance de travailleurs handicapés.

Dans le cadre de la journée internationale des droits des femmes, le SGDSN a signé l'accord sur l'égalité professionnelle entre les femmes et les hommes des services du Premier ministre. Cet accord met en lumière les actions déjà engagées au sein du SGDSN avec :

- les nominations équilibrées, marque de reconnaissance de l'expertise des femmes au plus haut niveau du secrétariat général ;
- l'intégration, depuis 2023, dans la campagne de revalorisation du régime indemnitaire, d'un critère supplémentaire relatif à l'égalité salariale entre les femmes et les hommes (titulaires et contractuels).

La fonction sécurité-sûreté, intégrée organiquement à la sous-direction des ressources humaines, a poursuivi sa dynamique de renforcement, avec la structuration dans chaque direction du réseau des officiers de sécurité, des réseaux de prévention et des correspondants du règlement général de la protection des données (RGPD).

Le détachement de gendarmerie s'est réorganisé en intégrant le service des estafettes. Par ailleurs, deux nouvelles conventions d'affectation temporaire des militaires de la gendarmerie ont été signées en fin d'année, l'une par le GIC et l'autre par le SGDSN.

Enfin, la qualité du dialogue social entre l'administration et les représentants du personnel doit être une nouvelle fois soulignée, avec des relations sereines et constructives, centrées sur les attentes des agents, qui permettent d'améliorer les conditions de travail et la qualité de vie de tous.

Séminaire « handicap » du 19 novembre 2024


Comité social d'administration du 3 juin 2024


Signature de l'accord sur l'égalité professionnelles entre les hommes et les femmes, le 8 mars 2024

+71	ETP : nombre d'emplois plafond créés au SGDSN en 2023 (schéma d'emplois)
100 %	du taux d'atteinte du schéma d'emplois au 31/12/2023
1 310,7	emplois travaillés (prise en compte du temps de présence et de la quotité de travail) constatés au 31/12/2024
7	réunions du comité social d'administrations
5	réunions de la formation spécialisée santé, sécurité et conditions de travail

L'ADMINISTRATION GÉNÉRALE ET LES FINANCES

Malgré la fermeture planifiée de la plate-forme de facturation Chorus en mai 2024, la sous-direction de l'administration générale et des finances a lancé une réorganisation interne d'ampleur qui a permis de centraliser et améliorer le suivi des dépenses, depuis l'expression du besoin jusqu'au paiement de la facture.

Dans un même souci d'efficacité et de rationalisation, la sous-direction a entamé une révision des procédures et circuits de gestion des déplacements, désormais en place dans la quasi-totalité des entités. 2024 a été également marquée par l'expérimentation de l'outil de demande d'achat « Chorus formulaire » auprès de certains services. Véritable enjeu d'efficacité, de traçabilité et de sécurisation du circuit de la dépense publique, l'extension de « Chorus formulaire » à l'ensemble du SGDSN sera effectif en 2025.
La sous-direction s'est attachée à se tourner vers l'avenir en structurant des projets de long terme.
La gestion des archives et de l'information constitue un enjeu stratégique pour le SGDSN. Soumises aux règles relevant du livre II du Code du patrimoine, une politique d'archivage a été définie pour permettre à notre institution de fixer un cadre clair pour la gestion des informations papier et numériques (détermination des durées de conservation en conformité avec la réglementation ou l'utilisation de l'information par les producteurs ; clarification des modalités de tri, de versement et d'élimination des documents NP et classifiées. Cette politique a été diffusée auprès des services et a été accompagnée d'un guide et de fiches de « bonnes pratiques » pour faciliter sa compréhension et son application. En 2024, la création d'un réseau de correspondants-archives a ainsi été constitué pour relayer les bonnes pratiques à l'ensemble des directions et assurer un premier niveau d'accompagnement sur les questions de gestion de l'information et de l'archivage. Un programme de sensibilisation et de formation leur a été proposé afin de garantir leur montée en compétences. Le bureau des archives s'est également investi dans les sensibilisations des nouveaux arrivants en lien avec la division sécurité-sûreté de SAG.

Formant une partie des archives de défense, les archives du SGDSN ont toujours fait l'objet d'un soin particulier. Saisi par les services d'archives pour toute demande de communication d'accès sur ses archives historiques, le SGDSN s'est également mobilisé à plusieurs reprises, lors des commissions d'accès et de déclassification, pour l'analyse et l'expertise des documents produits et reçus en vue d'en faciliter l'accès ou d'en protéger les informations conservées.

Mont-Valérien, inauguration du bâtiment 38, 1er février 2024

La croissance des effectifs entamée depuis une quinzaine d'année, combinée aux contraintes de la protection du secret de la défense nationale, génère des besoins structurels de surface de travail. Confronté à des coûts de location élevés pour une partie des emprises qu'il occupe et aux contraintes particulières des bâtiments anciens classés pour la partie patrimoniale, le SGDSN s'est engagé dans une démarche de rationalisation organisationnelle et budgétaire.
Ce travail passe par l'élaboration d'un schéma pluriannuel de stratégie immobilière, assurant une visibilité à court et moyen terme et planifiant la maintenance des installations techniques afin d'éviter toute rupture opérationnelle. Pour bénéficier d'une expertise dont il ne dispose pas, le SGDSN a passé une convention de maîtrise d'ouvrage déléguée à l'Opérateur du patrimoine et des projets immobiliers de la Culture en décembre 2024. Cette coopération permet de sécuriser techniquement et budgétairement la réhabilitation d'un des bâtiments de l'Hôtel national des Invalides. Ce chantier d'un montant de 13 millions d'euros sur 3 ans permettra de restaurer un bâtiment historique de 1 000 m² au bénéfice de près de 80 agents.

Enfin, l'année 2024 aura été marquée par la mise en perspective et l'inscription dans une trajectoire cohérente des actions de transition écologique du SGDSN. Le bilan des émissions de gaz à effet de serre en est la première étape, avant l'élaboration d'une feuille de route environnementale ambitieuse pour les prochaines années.

LES PERSPECTIVES 2025

▸ la mise en place de procédures et outils partagés avec les directions et les services ;

▸ le renforcement du pilotage de la masse salariale ;

▸ le développement d'un outil de gestion des formations transversales ;

▸ des chantiers immobiliers : l'inauguration et la mise en service d'un nouveau bâtiment, un chantier de rénovation d'une façade, la livraison de nouveaux modulaires et la conduite d'études visant à la remise en état d'un bâtiment historique du SGDSN.

241	millions d'euros de budget
10 400	demandes de paiement (+11 % par rapport à 2023)
3 450	engagements juridiques nouveaux (-5 % par rapport à 2023)
44	marchés publics lancés (+10 % par rapport à 2023)
6 400	ordres de mission traités (+14 % par rapport à 2023)
318	opérations logistiques
1,5	million de tirages réalisés par l'atelier impression
9 600	articles sélectionnés par le centre de documentation pour la réalisation de la revue de presse et des veilles particulières et une moyenne de 20 recherches documentaires par jour
27	mètres linéaires (ml) d'archives transférés au service historique des armées et 38,48 ml éliminés
13	millions d'euros en autorisations d'engagement et crédits de paiement pour la rénovation de 1000 m² au HNI
12 500	tonnes d'équivalent CO^2 émises en 2023 et calculées en 2024 (bilan carbone réalisé)

LINE BONMARTEL-COULOUME

Cheffe du service de l'administration générale

> Le SAG, avec la contribution active de l'ensemble des directions et services, a réalisé en 2024 le premier bilan des émissions de gaz à effet de serre.

Comment le SGDSN s'inscrit-il dans les engagements pour la transition écologique de l'État ?

La circulaire de la Première Ministre du 21 novembre 2023 relative aux services publics écoresponsables rappelle l'importance de l'exemplarité de l'État, et s'appuie sur le cap fixé par la stratégie bas-carbone, à savoir la neutralité carbone d'ici 2050. Définissant quinze engagements matérialisant le plan de transformation écologique de l'État, cette circulaire permet de prendre en considération les enjeux relatifs à la formation, aux déplacements, aux achats, au numérique responsable, aux déchets, à la consommation énergétique, aux bâtiments et à la préservation de nos écosystèmes. Elle rappelle aussi l'obligation, pour les services de l'État, de réaliser leur bilan des émissions de gaz à effet de serre, qui permet de quantifier les émissions et d'en établir un suivi.

De nombreuses actions ont déjà pu être menées en 2024 :

- quatre ateliers de sensibilisation sur les déplacements, le numérique responsable, la gouvernance de la transition écologique et les déchets d'équipements électriques et électroniques (DEEE) ;
- une boîte à idée autour des sujets de recyclage et de réemploi et l'ouverture d'un canal de discussion relatif à ces thématiques ;
- la mise à disposition de vélos pour les déplacements des agents ;
- le remplacement des ampoules par des ampoules basse consommation ;
- la suppression des gobelets à usage unique, *etc.*

Aussi, des démarches pour installer le tri sélectif sur l'ensemble de nos implantations et pour favoriser une meilleure valorisation de nos déchets d'équipements électrique et électronique (DEEE) ont été lancées. Afin de poursuivre et d'approfondir tous ces éléments, SAG, avec la contribution active de l'ensemble des directions, a par ailleurs réalisé sur 2024 le premier bilan des émissions de gaz à effet de serre (sur l'année de référence 2023). Regroupant l'ensemble de nos émissions directes et indirectes (à savoir la consommation énergétique, la production de froid, la quantité de déchets produits et leurs traitements, les déplacements quotidiens et professionnels des agents, l'ensemble des achats de biens et services, les immobilisations et les impressions), cet exercice nous aura permis d'obtenir notre profil carbone. En parallèle, une réflexion sur la résilience du SGDSN au changement climatique et son adaptation face aux risques induits a été engagée. ▸▸▸

La politique en faveur des personnes en situation de handicap est une priorité pour le gouvernement. Quelles actions ont été mises en œuvre au sein du SGDSN en 2024 ?

Depuis septembre 2023, le SGDSN a défini un plan d'actions, afin de favoriser l'inclusion des agents en situation de handicap et respecter l'obligation de taux d'emploi de 6 %, instaurée par la loi du 10 juillet 1987.

2024 constitue donc la 1ère année pleine de mise en œuvre de ce nouveau plan d'actions, avec, à la clef, l'atteinte des objectifs définis par la secrétaire générale du Gouvernement : 15 agents supplémentaires, nouvellement arrivés ou déjà en fonction et ayant effectué la démarche de reconnaissance, bénéficiant de l'obligation d'emploi ; soit 42 agents au total, au 31 décembre 2024, contre 27 un an plus tôt.

Les actions menées durant l'année écoulée se sont articulées autour de :

- l'information des agents du SGDSN sur les démarches à effectuer pour obtenir une reconnaissance en qualité de travailleur handicapé et à les accompagner dans leur carrière au sein du SGDSN ;

- la sensibilisation des managers au handicap, qu'ils soient déjà encadrants d'une personne en situation de handicap ou bien afin de les amener à considérer les candidatures de personnes RQTH, au même titre que toute autre candidature ;

- la sensibilisation plus largement de l'ensemble des personnels du SGDSN à la question du handicap, les différents échanges sur le sujet ayant démontré que d'importants biais cognitifs restaient présents.

Comment les rénovations lancées au sein de l'Hôtel national des Invalides s'inscrivent-elles dans la stratégie immobilière du SGDSN ?

Un des bâtiments du HNI, historiquement occupé par le SGDSN, va être rénové à partir de 2025. Compte tenu de la complexité de l'opération, l'Opérateur du patrimoine et des projets immobiliers de la Culture (OPPIC) va assurer la maîtrise d'ouvrage déléguée de l'opération. Il est spécialisé dans la construction ou la réhabilitation d'équipements culturels et dans la restauration et la valorisation de monuments historiques.

L'architecte en chef des monuments historiques (ACMH) est le maître d'œuvre de ce projet.

Les travaux permettront de réhabiliter un bâtiment historique de près de 1 000 m² pour y installer entre 75 et 85 personnes à échéance 2028. Le coût de ce projet d'ampleur est de 13 millions d'euros.

Après la phase d'étude et le lancement des appels d'offres en 2025, les travaux commenceront au printemps 2026 pour se terminer à l'été 2028. ◂

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