PREMIER
MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense
et de la sécurité nationale

RAPPORT D'ACTIVITÉ

RAPPORT D'ACTIVITÉ 2023

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 :
Stéphane Bouillon

Coordination :
Gwénaël Jézéquel

Conception et réalisation :
Louise Laurent

Coordination éditoriale :
Justine Boquet

SOMMAIRE

ÉDITO

Stéphane BOUILLON

Secrétaire général de la défense
et de la sécurité nationale

Une nouvelle fois, l'année passée a été copieuse. Au SGDSN, c'est souvent le cas, tant l'actualité et le contexte international pourvoient à l'agenda de chacune des composantes de l'ensemble. Néanmoins, l'année 2023 fut dense à bien des égards et a maintenu tout l'équipage sur le pont.

En 2023, les conflits ne se sont pas apaisés. Les zones d'affrontement se sont même accrues. Si ces guerres peuvent sembler lointaines, les interdépendances, la mondialisation, la manière dont nous les appréhendons en font des sujets de notre travail quotidien. Elles ont des répercussions importantes sur la vie politique et sociale de notre pays, sur notre économie, notre sécurité. Certains de nos adversaires les exploitent pour exacerber la polarisation de notre société, semer le doute, faire naître des inquiétudes chez nos concitoyens.

Dans ce contexte, la mission dévolue à Viginum par le Président de la République prend tout son sens. Les campagnes de manipulations de l'information à l'encontre de la France se succèdent à rythme élevé et sont même en augmentation permanente. Au-delà d'un accroissement quantitatif, on constate également une amélioration qualitative de ces manœuvres tout à fait préoccupante. Les réseaux sociaux participent souvent de leur diffusion massive. Les nouvelles technologies, telles que l'intelligence artificielle, les crédibilisent. Le fait de veiller, détecter, analyser tous les comportements numériques inauthentiques provenant d'acteurs étrangers prend alors tout son sens et de beaux succès opérationnels sont à saluer. La campagne *RRN* révélée par Viginum, en est le meilleur exemple. Mais s'il faut saluer les succès, beaucoup de travail demeure à accomplir, notamment pour accroître la résilience informationnelle des Français face au retour des propagandes adverses.

Autre menace, les cyberattaques ne faiblissent pas et constituent un danger majeur, dans la perspective des élections européennes, et ensuite des jeux Olympiques et Paralympiques. La tentation de nos adversaires d'exploiter cet événement, festif, fédérateur et extrêmement médiatisé, pour semer le trouble sera grande. La résilience de nos infrastructures numériques est donc un sujet de premier plan. Le SGDSN s'y prépare depuis de nombreux mois. L'ANSSI a été désignée cheffe de file de la cybersécurité des jeux, afin de sécuriser les systèmes d'information, d'accompagner les acteurs « critiques » face à la menace et de prodiguer les bonnes pratiques en termes d'hygiène numérique.

Au côté des risques de cybersécurité, d'autres menaces planent sur nos intérêts fondamentaux, et pourraient venir malmener le déroulement des jeux de Paris. PSE, chef d'orchestre de la préparation de l'État aux crises, est sur le front depuis 2022. Des exercices ont été conduits, prenant en compte les menaces identifiées. La chaîne gouvernementale de gestion de crise, sous l'égide du Premier ministre, ▸▸▸

ÉDITO

Stéphane BOUILLON

Secrétaire général de la défense
et de la sécurité nationale

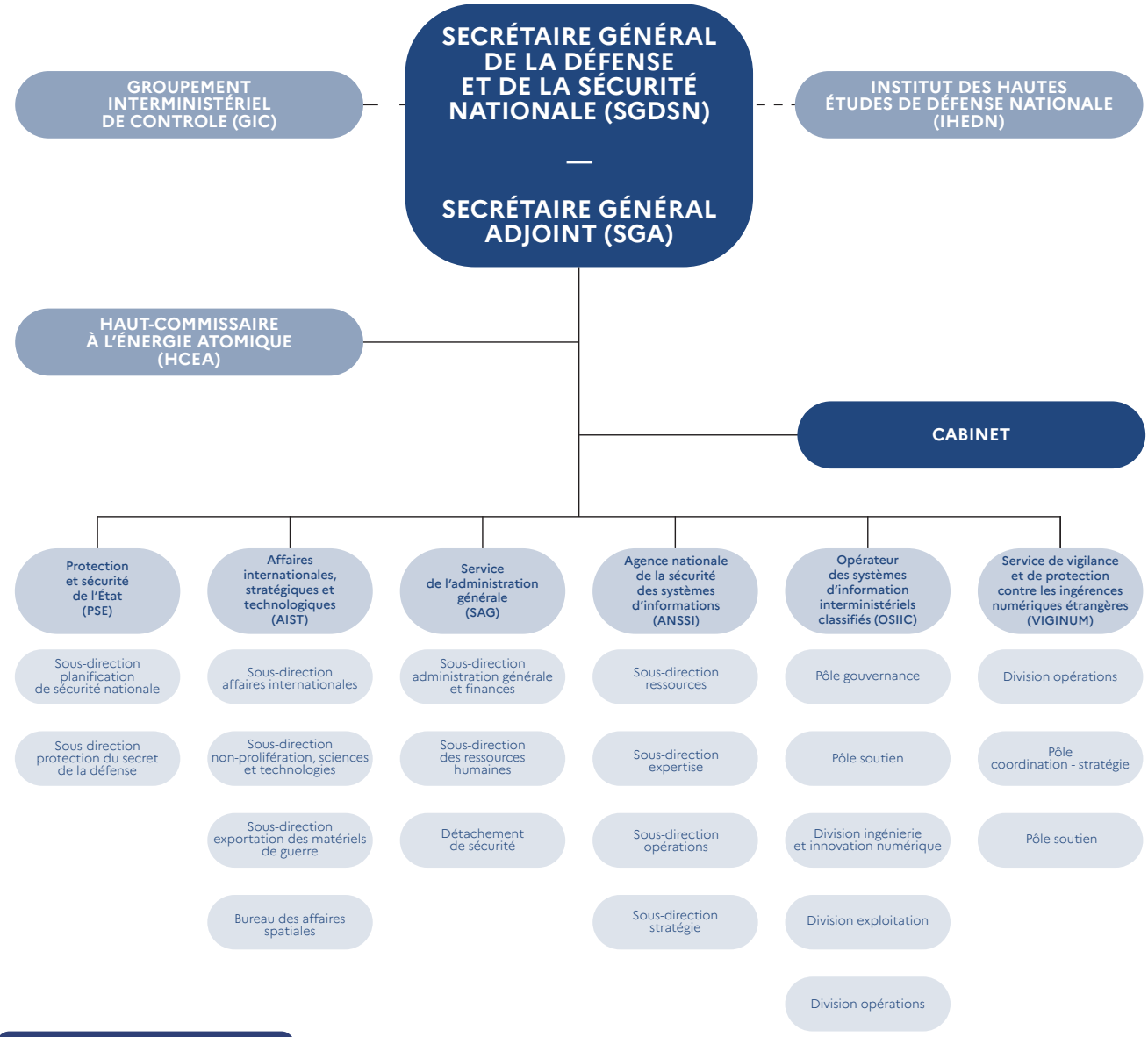
a été entraînée afin d'éprouver sa capacité à faire face, à se coordonner et à être en mesure d'assurer la résilience de la France. C'est aussi le sens des travaux d'anticipation stratégique conduits par AIST.

La préparation et la sécurisation d'événements exceptionnels sont venus s'ajouter à d'autres chantiers comme l'intégration de mesures de cybersécurité au sein de la LPM, qui vous seront présentées dans ce rapport, la poursuite des travaux de transposition des directives *REC*, *NIS 2* et *DORA*, qui concernent PSE et l'ANSSI directement, ou l'amélioration continue de la résilience de nos systèmes d'information et la mise en œuvre des moyens de communication classifiés de nos autorités, qui amènent l'OSIIC à conduire de nombreuses transformations numériques. Au-delà, le SGDSN a pris en compte de nouvelles missions, dont le secrétariat du conseil de politique nucléaire, par décret du Président de la République.

En matière de vie interne, le SGDSN s'est engagé en faveur de l'égalité, de la diversité et pour la qualité de vie au travail afin d'offrir un environnement répondant aux attentes de nos agents. Il s'est mobilisé, aussi, pour la transition écologique.

Vous trouverez le détail des temps forts qui ont rythmé cette année en parcourant ce rapport d'activité. Mais quels que soient les aléas, depuis le début du XX^{e} siècle, nos missions n'ont en réalité pas beaucoup changé : auprès du Premier ministre, en liaison étroite avec la Présidence de la République, nous coordonnons l'action gouvernementale dans le domaine de la sécurité et de la défense, nous faisons travailler ensemble les ministères, les établissements publics, les opérateurs privées et publics d'importance vitale. Nous nous adaptons à l'évolution de la menace et des risques quels qu'ils soient. Nous agissons, nous anticipons, nous planifions, nous préparons l'avenir. C'est la raison d'être du SGDSN, qui nonobstant le temps, les réformes et les épreuves auxquels notre pays est confronté, continue de regarder vers l'avant afin d'appréhender les défis de demain. ◂

ORGANIGRAMME



Effectifs au 31/12/2023

CAB :	26	ANSSI :	666
PSE :	66	OSIIC :	287
AIST :	62	GIC :	318
SAG :	105	VIGINUM :	43

ÉLÉMENTS DE CHRONOLOGIE 2023

19 JANVIER
La Première ministre, Elisabeth Borne installe Vincent Strubel comme directeur général de l'ANSSI

19 JANVIER
Session plénière du dialogue spatial bilatéral franco-japonais

14 MARS
Exercice Lutetia

20 MARS
Activation de la CIC « approvisionnement en carburant » (13 réunions)

27–28 MARS
Mission du SGA à Londres

29 MARS
Activation de la CIC « sécheresse » (10 réunions)

30 MARS
Le SGDSN accueille la phase 3 de l'exercice ORION

21–22 MARS
Atelier interdisciplinaire sur la sécurité globale, coorganisé par l'ANR, le MESRI et le SGDSN

4 AVRIL
Présentation du projet de loi de programmation militaire en conseil des ministres

10 AVRIL
Publication du guide de bonnes pratiques sur le transfert de flux dits « intangibles »

14 AVRIL
Inauguration du *hub* logistique interministériel de Marseille

24-27 MAI
Mission du SGA à Dakar

31 MAI
Le SG reçoit le ministre coordinateur de la sécurité nationale de Singapour

7 JUIN
Parution du livre *Au cœur de l'État : une histoire du Secrétariat général de la défense et de la sécurité nationale*

7 JUIN
Yves Verhoeven est nommé directeur de l'OSIIC en conseil des ministres

13 JUIN
Publication du rapport *RRN, une campagne numérique de manipulation de l'information complexe et persistante*

13-14 JUIN
Mission du SG en Allemagne

19-23 JUIN
Exercice *Handspinner*

20 JUIN
Forum consacré à la lutte contre les manipulations de l'information, organisé par Viginum

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

21 JUIN
Posture « Été-automne 2023 » du plan Vigipirate (sécurité renforcée – risque attentat)

26 JUIN
Publication du premier rapport du comité éthique et scientifique de Viginum

27 JUIN
Commission interministérielle de sécurité aérienne (CISA)

29 JUIN
Activation de la CIC «violences urbaines» (11 réunions)

5 JUILLET
Séminaire cyber JOP24

6 JUILLET
Séminaire franco-allemand sur les menaces hybrides

11-12 JUILLET
Exercice CNCS - CIC

C4

18 janvier
13 février
20 mars
25 avril
19 juin
19 juillet
18 septembre
16 octobre
23 novembre

17 AOÛT
Activation de la CIC « canicule » (2 réunions)

23 AOÛT
Activation de la CIC « pénurie d'eau à Mayotte » (8 réunions)

4–5 SEPTEMBRE
Mission du SGA en Estonie

21 SEPTEMBRE
Signature par la secrétaire générale du Gouvernement d'une convention de partenariat entre les services de la Première ministre et La Cordée, visant à promouvoir la diversité au sein du service public

1ER OCTOBRE
Prise de poste de Mme Line Bonmartel-Couloume en tant que cheffe du service de l'administration générale

2 OCTOBRE
Début du déploiement du Secdroid 11

4 OCTOBRE
Nomination de Marc-Antoine Brillant en tant que chef du service de vigilance et de protection contre les ingérences numériques étrangères

11 OCTOBRE
Nomination de Muriel Nguyen en tant que directrice de la protection et de la sécurité de l'État en conseil des ministres

13 OCTOBRE
Élévation du plan Vigipirate au niveau « urgence attentat » et densification de la posture en cours

17-18 OCTOBRE
4ème édition du *SAFE Seminar* consacré à la lutte anti-drones, Le Castellet

17 OCTOBRE
Mission du SG à l'OTAN

31 OCTOBRE
Nomination de Caroline Ferrari en tant que directrice des affaires internationales, stratégiques et technologiques en conseil des ministres

4–8 NOVEMBRE
Mission du SGA au Qatar

13 NOVEMBRE
Activation de la CIC « inondations dans le département du Pas-de-Calais » (1 réunion)

17-20 NOVEMBRE
Mission du SG à Bahreïn

22 NOVEMBRE
Inauguration du bâtiment ArteFact, antenne rennaise de l'ANSSI

21 NOVEMBRE
Organisation par le SGDSN, dans le cadre de la SEEPH, d'un séminaire consacré au management inclusif

4 DÉCEMBRE
Mise en ligne de la nouvelle plateforme *Je clique ou pas ?*

5-6 DÉCEMBRE
Exercice JOP

13 DÉCEMBRE
Commission interministérielle de sécurité aérienne (CISA)

18 DÉCEMBRE
Exercice Énergie

13 AU 17 DÉCEMBRE
Mission du SGA aux États-Unis

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

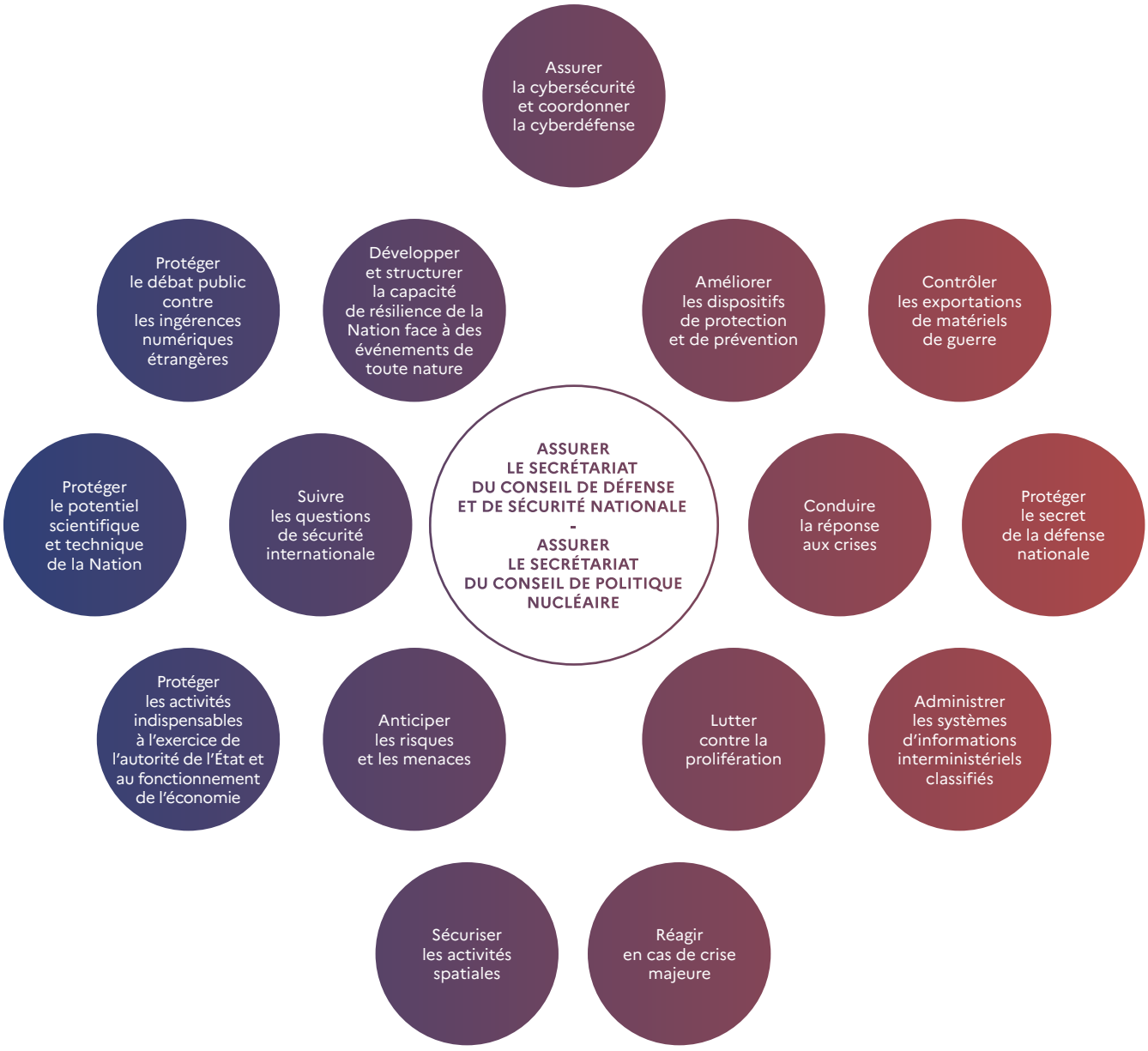
COLMI

9 février
17 mars
21 avril
26 mai
7 juillet
3 octobre
3 novembre
20 décembre

COLISÉ

8 février (Colisé opérationnel)
12 avril (Colisé opérationnel)
5 juillet (Colisé plénier)
18 octobre (Colisé opérationnel)
6 décembre (Colisé plénier)

LES GRANDES MISSIONS DU SGDSN



ASSURER LA CYBERSÉCURITÉ ET COORDONNER LA CYBERDÉFENSE

Retour sur les mesures cyber de la loi de programmation militaire

Loi de référence visant à fixer à la fois les grandes orientations de défense pour la période 2024 – 2030 et les volumes budgétaires alloués aux armées sur la période, la loi de programmation militaire a aussi occupé une partie des équipes du SGDSN, notamment par son chapitre V.

Le 1er août 2023 a été promulguée la loi n° 2023-703 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense. Document de référence faisant suite aux conclusions de la revue nationale stratégique, la LPM couvre de multiples domaines, à la fois géostratégique, capacitaire, industriel, financier ou encore les conditions de vie et de travail des personnels de la défense. Planifiant les orientations de défense pour six ans, la LPM vise à doter les armées de moyens à la hauteur du contexte national et international, marqué par un retour de la guerre de haute intensité et par l'imbrication des crises.

Indépendamment de la programmation budgétaire du ministère des armées et des mesures normatives intéressant la défense militaire, comme en 2013 et en 2018, un chapitre voué à la cybersécurité a été intégré à la LPM. Le projet de loi précise qu'il s'agit de « *permettre à l'ANSSI d'accroître sa connaissance des modes opératoires des cyberattaquants, de mieux remédier aux effets de leurs attaques et d'alerter plus efficacement les victimes des incidents ou des menaces pesant sur leurs systèmes d'information* ». Quatre articles mettent en œuvre ces objectifs – trois portant de nouvelles dispositions et un venant renforcer un dispositif introduit par la LPM précédente, inséré dans le code de la défense et le code des postes et des communications électroniques (CPCE). Un cinquième article, introduit par les parlementaires, organise l'information publique sur l'application de certaines mesures.

Dans le détail, l'article 64 permet désormais à l'ANSSI de prescrire des mesures de filtrage des noms de domaine aux acteurs du *Domain name system* (DNS), le système de correspondance entre une adresse « machine » et un nom de domaine, afin de neutraliser une utilisation dévoyée de celui-ci par un cyberattaquant et ainsi de mieux comprendre ses modes opératoires.

Cette disposition est conçue selon une logique graduelle. Une distinction est ainsi faite selon que le nom de domaine est ▸▸▸

enregistré de bonne foi par son propriétaire légitime ou enregistré dans le seul but de commettre une cyberattaque. Le propriétaire de bonne foi est invité à prendre des mesures de remédiation. En cas d'inaction, l'ANSSI intervient en demandant la suspension ou le blocage du nom de domaine. Si le nom de domaine est enregistré aux seules fins d'une cyberattaque, au-delà des mesures mentionnées, l'ANSSI peut demander la redirection du nom de domaine vers un serveur neutre ou sécurisé. La redirection vers un serveur sécurisé permet à l'ANSSI de recueillir des données sur le mode opératoire du cyberattaquant. Cette dernière mesure est entourée de garanties fortes puisque la phase d'observation ne dure que deux mois et ne peut être renouvelée qu'après accord de l'ARCEP.

L'article 65 permet à l'ANSSI d'obtenir la communication automatique, par les opérateurs, de données anonymisées contenues dans les caches DNS, afin d'identifier les vecteurs et serveurs par lesquels transite une attaque informatique. Les données recueillies permettront à l'agence d'enrichir la base de connaissance de la menace et de renforcer ses capacités de détection vis-à-vis des comportements malveillants.

Les dispositions de l'article 66 obligent désormais les éditeurs de logiciels à communiquer à leurs utilisateurs et à l'ANSSI les vulnérabilités identifiées dans leurs produits ou les incidents visant leurs systèmes d'information ayant une incidence sur leurs produits. La transparence du marché des logiciels est ainsi renforcée et permet aux utilisateurs de mettre en place les mesures de remédiation adaptées.

L'article 67 se décline en trois composantes venant respectivement modifier les articles L. 2321-2-1 et L. 2321-3 du code de la défense, ainsi que L. 33-14 du CPCE.

La première composante vient :

- étendre les données recueillies au contenu des communications qui transitent par les réseaux et, plus largement, permettre à l'ANSSI d'obtenir la copie du serveur utilisé par l'attaquant ;
- inclure les opérateurs de centres de données *(cloud)* dans le périmètre des opérateurs concernés par les marqueurs techniques ou la copie de serveurs ;
- inclure les sous-traitants des autorités publiques, des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE) au profit desquels l'ANSSI peut détecter et caractériser des événements susceptibles d'affecter la sécurité de leurs systèmes d'information.

La seconde composante oblige les opérateurs de communications électroniques (OCE) qui sont OIV à se doter de capacités de détection.

La troisième composante, enfin, étend aux hébergeurs de données l'obligation de communication de l'identité et de l'adresse d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, et élargit le périmètre de cette communication aux données techniques des sous-traitants des OIV, OSE et autorités publiques.

L'article 68 de la loi, enfin, fait obligation à l'ANSSI de faire annuellement rapport au Parlement de l'application des mesures figurant désormais à l'article L. 2321-2-3 du code de la défense. ◂

RENFORCER LES CAPACITÉS DE PROTECTION DE L'ÉTAT

CONTRIBUER À LA SÉCURITÉ DES GRANDS ÉVÉNEMENTS ET RENFORCER LA CAPACITÉ DE L'ÉTAT À RÉPONDRE À DES CRISES MAJEURES

En 2023, la direction PSE a intensifié son action au bénéfice des ministères impliqués dans la préparation des grands événements sportifs : coupe du monde de rugby 2023 (CMR 2023) et jeux Olympiques et Paralympiques de Paris 2024 (JOP24). Elle a ainsi poursuivi et actualisé ses travaux de préparation de l'État aux crises, notamment par l'organisation d'exercices et de formations. Elle a également engagé un important travail de planification sur la résilience des réseaux et veillé à la cohérence des initiatives menées en matière de lutte anti-drones (LAD) et de protection dans le domaine nucléaire, radiologique, biologique, chimique et explosifs (NRBC-E). Enfin, la direction PSE a finalisé son cycle d'expérimentations en matière de technologies de sécurité.

Par ailleurs, et de manière plus générale, la direction a poursuivi sa mission de préparation des Conseils de défense et de sécurité nationale (CDSN).

L'ARTICULATION ET LA PROFESSIONNALISATION DES ACTEURS

En charge de la préparation de l'État à la gestion des crises majeures, le bureau de préparation de l'État aux crises (BPEC) a été fortement mobilisé avec l'organisation de la coupe du monde de rugby à l'automne 2023 et la préparation des JOP24. Un important travail doctrinal a été engagé en 2023 afin de réviser la circulaire du Premier ministre relative à l'organisation gouvernementale pour la gestion des crises majeures, désormais disponible sur Légifrance. Par ailleurs, les référentiels opérationnels de la cellule interministérielle de crise (CIC) et du centre national de commandement stratégique (CNCS) ont été validés au début de la coupe du monde de rugby. Les travaux menés par le SGDSN ont permis d'introduire ce nouvel acteur au sein des organes de gestion de crise et tout particulièrement en lui donnant la mission d'accueillir en son sein la CIC en cas de crise pendant les grands événements sportifs internationaux (GESI).

Poursuivant la préparation spécifique des centres opérationnels nationaux, deux exercices de crise majeure ont permis de tester les dispositifs de sécurité. Après l'exercice RUGBY22, joué les 29 et 30 novembre 2022 et portant sur une attaque NRBC, la direction PSE a testé, les 11 et 12 juillet 2023, l'insertion et l'articulation du CNCS avec la chaîne de commandement. En 2023, un dernier exercice portant sur la capacité de l'État à faire face à une cyberattaque majeure ayant des effets sur la cérémonie d'ouverture des JOP et l'organisation des transports en commun, a été réalisé les 5 et 6 décembre (exercice JOP 23).

La direction PSE a contribué à l'organisation de la coupe du monde de rugby en assurant une présence au CNCS lors des journées d'activation du centre en posture de « suivi renforcé ». Outre la mission d'appui méthodologique, les agents de la direction ont mené des travaux d'anticipation opérationnelle et ont contribué au retour d'expérience sur l'organisation de la coupe du monde de rugby.

Enfin, le cycle de formation a été poursuivi, notamment à travers le programme de professionnalisation des acteurs de la gestion de crise (PAGC) porté par le SGDSN depuis 2019. En 2023, ce cycle a permis d'entraîner environ 400 personnes susceptibles d'être mobilisées en CIC et dans les centres opérationnels ministériels.

LE SUIVI SECTORIEL ET LA COORDINATION INTERMINISTÉRIELLE DES MESURES DE SÉCURISATION DES GRANDS ÉVÉNEMENTS

LES TECHNOLOGIES DE SÉCURITÉ

La direction PSE a finalisé le cycle des expérimentations de sécurité, conduites depuis 2019 en partenariat avec la Coordination nationale pour la sécurité des JOP24 et des grands événements sportifs internationaux (CNSJ), ainsi qu'avec le Comité stratégique de la filière des industries de sécurité (CFS-IS) dont la maîtrise d'ouvrage avait été confiée au pôle de compétitivité SAFE-CLUSTER.

Une dernière expérimentation a été conduite en août 2023 au stade Orange Vélodrome pour évaluer les capacités de détection de deux équipements français de scanners millimétriques pour le contrôle d'accès sur les personnes. Le déploiement de ces équipements a été rendu possible à la suite de l'adoption de la loi du 19 mai 2023 relative aux jeux Olympiques et Paralympiques 2024. Le retour d'expérience de cette expérimentation a été présenté en octobre aux ministères et opérateurs, dont l'organisateur Paris 2024.

LA LUTTE ANTI-DRONES

Les travaux interministériels de lutte anti-drones (LAD) ont été poursuivis et renforcés en 2023 dans la perspective de l'organisation des grands événements sportifs : analyse de la menace ; évaluation de la vulnérabilité des sites concernés par la coupe du monde de rugby 2023 et les jeux Olympiques et Paralympiques 2024 ; identification des besoins en moyens de protection ; développement capacitaire de la LAD et renforcement du cadre juridique de la lutte anti-drones. Deux commissions interministérielles de sûreté aérienne (CISA) ont permis de rendre compte de l'avancée de ces actions au cabinet du Premier ministre.

La direction a également contribué financièrement à la réalisation d'un important exercice de lutte anti-drone (COUBERTIN LAD) conduit en janvier 2023 par le ministère des armées. L'exercice a permis de valider les principes d'intégration des moyens dans le contexte interministériel (interconnexion des systèmes, architecture de commandement, outil de supervision…) mis en œuvre avec succès à l'occasion de la CMR 2023 mais également dans la perspective des JOP24.

Enfin, deux textes ayant fait l'objet d'une coordination interministérielle assurée par la direction PSE sont entrés en vigueur en 2023 : le décret du 27 mars 2023 relatif au brouillage des drones et l'article 58 de la loi du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 pour la partie concernant la neutralisation des drones menaçants.

LA LUTTE CONTRE LA MENACE NRBC-E

Présidé par le SGDSN, le comité stratégique NRBC-E a permis de suivre l'évolution du programme interministériel d'action (PIA) NRBC-E 2021-2023 et de préparer le programme 2024-2027 du contrat capacitaire interministériel de lutte contre le terrorisme NRBC (CCI NRBC).

Après avoir remporté un appel à projet européen *RescUE stockpilling NRBC* en 2022 pour 166 millions d'euros d'achat d'équipements NRBC, l'année 2023 a été marquée par un second appel à projet européen : *RescUE stockpilling NRBC* et pandémies. La France a été retenue pour un montant de 210 millions d'euros d'achat d'équipements NRBC entreposés en France. Ces moyens européens ont, pour partie, été utilisés lors de la CMR 2023 et le seront à nouveau pour les JOP24.

LA LUTTE CONTRE LES EXPLOSIFS

Le centre de certification des unités cynotechniques privées pour la recherche d'explosif, initié par la direction PSE, dorénavant piloté par la direction générale de la police nationale (DGPN), a ouvert ses portes à Biscarrosse le 1er janvier 2023. Plusieurs textes réglementaires préparés en 2022 (décret encadrant les unités déployées par les opérateurs d'événementiel et de sites sensibles, arrêté fixant les modalités d'intervention et de formation initiale, *etc.*) ont été publiés au début de l'année 2023 afin d'encadrer les modalités de certification de ces unités.

LA RÉSILIENCE DES RÉSEAUX

En appui aux ministères, dans le cadre de la mise en œuvre de la planification sectorielle qui leur incombe, la direction PSE a conduit un cycle de réunions visant à assurer la sécurisation de l'alimentation électrique durant les JOP24. Ces travaux ont été progressivement élargis à la téléphonie mobile et aux moyens de paiement afin de veiller à la bonne prise en compte des menaces pouvant peser sur ces secteurs.

Par ailleurs, des travaux ont été menés sur la protection des réseaux d'eau et de la chaîne alimentaire avec les ministères en charge de l'agriculture, de la santé, de l'économie et de la transition écologique.

METTRE EN ŒUVRE LA STRATÉGIE NATIONALE DE RÉSILIENCE (SNR) ET PROMOUVOIR UNE POLITIQUE DE SOUVERAINETÉ

Validée par le cabinet de la Première ministre le 21 avril 2022, la stratégie nationale de résilience (SNR) est entrée dans sa phase opérationnelle en 2023. Ce document stratégique est constitué de 3 axes : préparation de l'État aux crises ; renforcement des ressources humaines et matérielles ; adaptation de la communication publique. Des actions opérationnelles déclinent ces axes. Les ministères rendent compte de l'avancée des actions dont ils ont la charge à l'occasion du Comité interministériel pour la résilience nationale (CIRN) créé en 2023 pour assurer un portage politique à haut niveau. Présidé par le directeur de cabinet du Premier ministre, ce comité s'est réuni à deux reprises (1er février et 6 octobre 2023).

L'année 2024 sera l'occasion de faire un premier bilan des actions du CIRN et d'identifier de nouveaux axes prioritaires, adaptés au contexte géopolitique et sécuritaire d'aujourd'hui.

LA CONTINUITÉ DES MISSIONS ESSENTIELLES

LE DIALOGUE CIVILO -MILITAIRE

Dans le cadre des travaux relatifs à la SNR, le SGDSN a organisé avec l'état-major des armées (EMA) la phase 3 de l'exercice ORION. La restitution de cet exercice a eu lieu le 30 mars 2023, sous la présidence du directeur de cabinet de la Première ministre[1].

Associant l'ensemble de la communauté interministérielle, l'exercice ORION 3 a permis de préparer les services de l'État à un scénario paroxystique, éprouvant notre capacité à contenir une stratégie hybride d'un puissant compétiteur et nécessitant la mise en œuvre d'une coordination civilo-militaire renforcée.

Les conclusions de l'exercice ORION 3 ont contribué à l'élaboration de la feuille de route de la commission interministérielle relative à la défense nationale (CIDN) chargée d'animer la coordination des activités de défense civile et militaire sur l'ensemble des champs ministériels pour renforcer les capacités de l'État à gérer des crises majeures et surmonter les difficultés liées à des chocs éventuels. Ces travaux s'inscrivent en cohérence avec les orientations arrêtées par le CIRN.

200 participants

5 groupes de travail thématiques

LA CONTINUITÉ DE L'ACTION DE L'ÉTAT

La direction PSE a piloté en 2023 le premier comité de suivi pour la continuité du travail gouvernemental. Présidé par le cabinet du Premier ministre, son objet est de s'assurer de l'aptitude des ministères à mettre en œuvre la continuité du travail gouvernemental quels que soient les événements perturbateurs susceptibles de survenir, dans une approche multirisques. Les travaux menés par ce comité sont en lien avec ceux du comité interministériel pour la résilience nationale (CIRN).

La direction a également édité le guide en ligne de la continuité d'activité en mars 2023. Une mise à jour du site est actuellement en cours.

[1] L'objectif du cycle d'exercices d'ORION 23 est de renforcer la préparation opérationnelle interarmées dans le cadre d'une opération d'envergure. Ce cycle comprend quatre phases : 1. Planification opérationnelle, 2. Entrée en premier, 3. Travaux interministériels, 4. Opération d'envergure. L'implication du SGDSN dans la phase 3 fait suite à une sollicitation du ministère des armées formulée le 15 novembre 2021 parallèlement à l'élaboration de la stratégie nationale de résilience.

LA RÉSILIENCE DU MONDE ÉCONOMIQUE

LA TRANSPOSITION DE LA DIRECTIVE RÉSILIENCE DES ENTITÉS CRITIQUES

La direction PSE a été fortement mobilisée par les travaux préparatoires à la transposition de la directive sur la Résilience des Entités Critiques (REC), négociée sous présidence française de l'Union Européenne (PFUE), qui conduira à une modernisation du dispositif de sécurité des activités d'importance vitale (SAIV).

La modification du dispositif SAIV exigée par la directive permet au SGDSN de réformer en profondeur le dispositif national existant, afin d'intégrer pleinement la logique de résilience promue par le texte européen et renforcer la coordination européenne sur ce sujet.

A ce titre, la direction PSE a piloté plus de 30 réunions de travail avec les différentes administrations en charge de la SAIV – ministères coordonnateurs, zones de défense et de sécurité, préfectures de département, services enquêteurs – afin d'identifier les modifications à apporter au dispositif actuel. Elle a également participé aux négociations de textes européens connexes, tels que ceux organisant la coordination européenne en cas d'incident majeur sur une infrastructure critique ayant un impact transfrontière.

LES STOCKS STRATÉGIQUES

Après une phase d'échanges interministériels sur la nature des réserves à constituer ayant abouti à la distinction entre « biens vitaux » et « biens souverains », la direction a produit une matrice de recension des besoins, diffusée à l'ensemble des départements ministériels. Cette première étape de recension partielle a été présentée à l'occasion du CIRN2, le 6 octobre 2023. Ce travail se poursuit afin d'aboutir à un niveau de précision suffisant pour présenter aux autorités politiques les arbitrages budgétaires subséquents.

LA MOBILISATION DES TERRITOIRES

L'IMPLICATION DES CITOYENS

La SNR met un accent particulier sur la sensibilisation et la responsabilisation du citoyen. L'un des enjeux est notamment de développer la préparation de la population à la crise. Cela regroupe différentes actions allant de la mobilisation des citoyens dans les dispositifs d'engagement, au renforcement de la formation sur les comportements à adopter (gestes de premier secours, confinement, faire face ensemble, kit d'urgence, hygiène numérique…) jusqu'à la modernisation des dispositifs d'alerte et d'information des populations en situation de crise. Plusieurs axes de travail concrets participent à cet objectif : l'élaboration du Plan Individuel de Mise en Sûreté (PIMS), l'organisation de la journée nationale de la résilience (JNR), la rationalisation de l'information sur les risques et menaces (portail www.info.gouv.fr/risques), ou encore le travail mené sur la structuration des viviers de réserves citoyennes et leur valorisation, en lien avec la Garde nationale.

LES COLLECTIVITÉS TERRITORIALES

A l'issue des rencontres avec les principales associations d'élus (AMF, ADF, Régions de France, France Urbaine…), est apparu un besoin de sensibilisation des élus et fonctionnaires à la SNR, ainsi que l'instauration d'un lieu de partage des bonnes pratiques.

Lors du CIRN2 du 6 octobre, il a été décidé de réaliser des parcours de présentation de la SNR (par le CNED pour les élus, par la DGAFP pour les fonctionnaires).

Un travail sur les relations maire-préfet a été lancé notamment en vue d'une coopération sur l'écriture des plans communaux de sauvegarde (PCS) et la réalisation d'exercices.

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

LA REFONTE DU CORPUS RÉGLEMENTAIRE

La sous-direction de la protection et de la sécurité de la défense nationale (PSD) chargée tout particulièrement du suivi de la politique de protection du secret de la défense nationale (PSDN) a engagé plusieurs actions dans le prolongement de la réforme concernant notamment la nouvelle instruction générale interministérielle n° 1300 (IGI 1300) entrée en vigueur en juillet 2021.

Sur le plan national, ces actions se sont accentuées afin que les différents acteurs, officiers de sécurité du public et du privé notamment, soient sensibilisés aux enjeux de cette politique publique et formés aux nouvelles mesures de protection du secret.

LE RENFORCEMENT DES OUTILS DE PILOTAGE ET D'ANIMATION DE LA POLITIQUE DE PROTECTION DU SECRET DE LA DÉFENSE NATIONALE

Le SGDSN a renforcé l'animation de son réseau de fonctionnaires de sécurité de défense (FSD) placés auprès de chaque haut fonctionnaire de défense et de sécurité (HFDS). Il a ainsi accompagné chaque ministère dans la déclinaison de la nouvelle IGI 1300 : élaboration des fiches pratiques sur la mise en œuvre de la PSDN à destination des personnes habilitées et des officiers de sécurité, formation de ces derniers avec l'institut des hautes études du ministère de l'intérieur (IHEMI).

La direction PSE a par ailleurs poursuivi et accentué sa mission de contrôle de l'application de la réglementation et du niveau de protection des informations les plus sensibles. Sept missions d'inspection ont ainsi été réalisées en 2023.

2 **inspections** menées en France au titre de la protection des ISC de l'OTAN/UE par le *NATO Security Office* (19-21 juin 2023) et par le SGC (28-30 novembre 2023), **8 sites** visités

7 **inspections** réalisées par la sous-direction PSD au titre du contrôle de la règlementation des ISC au niveau Très Secret faisant l'objet de classifications spéciales

LA GARANTIE DES ÉCHANGES DE DOCUMENTS CLASSIFIÉS AU NIVEAU EUROPÉEN ET INTERNATIONAL

Sur le plan international, la sous-direction a souhaité renforcer la révision des accords généraux de sécurité (AGS), enjeu majeur à l'international, notamment par la création, en septembre 2023, du bureau des affaires internationales et européennes (BAIE), l'élaboration d'un processus de priorisation et de dynamisation des négociations, l'identification des difficultés juridiques et des instruments pour y remédier, au plus près des partenaires bilatéraux et multilatéraux et en lien étroit avec les acteurs interministériels (MINARM et MEAE en particulier).

L'année 2023 a vu également la France être inspectée au titre du dispositif de sécurité mis en œuvre pour la protection des informations et supports classifiés (ISC) OTAN/UE, respectivement par le bureau de sécurité de l'OTAN (NATO Security Office – NOS) et par le Secrétariat général du Conseil (SGC) de l'Union européenne accompagné d'experts de la Commission européenne (dernière inspection en 2016 pour le premier organisme et en 2015 pour le deuxième). La sous-direction est intervenue en appui de cette inspection qui s'est déroulée de manière satisfaisante sur huit sites (ministère des affaires étrangères et européennes, secrétariat général des affaires européennes, *etc.*).

MURIEL **NGUYEN**

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

« La préparation aux crises a dû intégrer de nouveaux acteurs et s'adapter à l'évolution des risques et des menaces pour renforcer la capacité d'anticipation, l'aide à la décision des autorités et la résilience de la Nation. »

Comment résumeriez-vous le rôle et le positionnement de la direction au cours de l'année écoulée ?

La direction a dû autant mobiliser les outils utiles aux autorités pour la gestion des crises et la sécurisation des événements que préparer dans la durée de nouvelles réponses pour renforcer la résilience collective de la Nation et protéger nos intérêts fondamentaux. Son action s'est donc efforcée de conjuguer le temps court des réunions du conseil de défense et de sécurité nationale et des cellules interministérielles de crise, dictées par une actualité nationale et internationale sans répit, avec le temps long de l'anticipation, de l'analyse et de la planification dans le cadre d'une approche plus globale des risques et des menaces. Ces missions ont amené la direction à se positionner autant en Conducteur de sécurité sécurité défense pour apporter appui et expertise aux autorités qu'en coordonnateur et animateur du travail interministériel sans lequel il ne peut y avoir de réponses intégrées fédérant toutes les politiques publiques concourant à la résilience et associant tous les acteurs.

Quels ont été les principaux enseignements de l'année 2023 ?

Tout d'abord, le renforcement de la capacité de l'État à répondre à des crises majeures nécessite d'apprendre à coopérer avec de nombreux acteurs non-étatiques et à appréhender d'autres écosystèmes pour les intégrer aux schémas de prise de décision et de communication. Ensuite, la pression des événements et la complexité de l'environnement conduisent à prendre davantage en compte les besoins et les contraintes des autorités dans la méthode et les outils de planification avec pour objectif de faciliter la prise de décision et d'offrir plus de lisibilité. Par ailleurs, la continuité des missions essentielles à la vie de la Nation exige d'embarquer les entreprises, les collectivités locales et la société civile dans la stratégie nationale de résilience à l'heure où l'ampleur des interdépendances doit accélérer la recherche de solutions de souveraineté. Enfin, les équipes sont de plus en plus confrontées à un enjeu de conciliation entre un haut niveau d'expertise et un besoin d'accessibilité des réponses à apporter ce qui demande une forte capacité d'adaptation.

ANTICIPER, ÉVALUER, PROTÉGER, COOPÉRER AVEC NOS PARTENAIRES

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 2023, trois études majeures ont été menées dans le cadre du CIA et diffusées aux ministères ; plusieurs autres ont été lancées. 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. 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

L'année 2023 aura vu une multiplication des attaques hybrides contre nos intérêts et ceux de nos alliés et partenaires. Elle aura conforté la nécessité de lutter contre ces stratégies.

En ce domaine, les travaux interministériels sont animés par le SGDSN dans le cadre d'un groupe de travail permanent qui s'est réuni trois fois en 2023. Ils ont notamment permis d'évaluer les effets en matière hybride du conflit en Ukraine, afin de renforcer notre vigilance et notre résilience collectives. Cette capacité à la fois conceptuelle et opérationnelle du SGDSN en fait un pôle d'excellence reconnu et l'interlocuteur privilégié de nos alliés sur ce sujet, aussi bien dans les formats multilatéraux (notamment le groupe horizontal du conseil de l'UE sur les menaces hybrides) que bilatéraux. Ainsi, en 2023, 31 événements internationaux ont été consacrés à la question des réponses apportées aux menaces hybrides.

Enfin, le SGDSN assure l'interface entre l'interministériel et la cellule de fusion hybride du centre de situation et de renseignement de l'UE dans l'identification des grandes tendances annuelles de l'hybridité, et représente la France au sein du centre d'excellence d'Helsinki sur les menaces hybrides, un cercle de réflexion et de formations ouvert aux membres de l'UE et de l'OTAN.

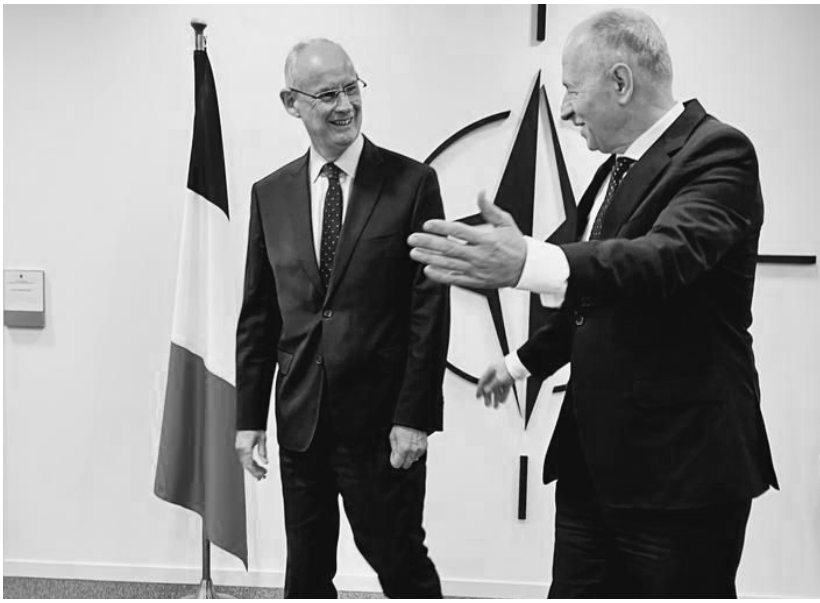
LUTTE CONTRE LE FINANCEMENT DU TERRORISME

En 2023, le SGDSN a continué de jouer un rôle de premier plan dans 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 avec la CNRLT le secrétariat exécutif, a confirmé en 2023 son rôle central en la matière : au 31 décembre 2023, 576 mesures de gel des avoirs pour motif de terrorisme étaient en vigueur sur le territoire national. Le GABAT implique 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 2023, suite aux recommandations du GAFI (groupe d'action financière internationale) et la doctrine GABAT a été actualisée en conséquence.

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 la nôtre (*National Security Advisor* ou *National Security Council*, par exemple). Le SGDSN s'implique sur les questions de sécurité au sein des instances multinationales (UE, OTAN) ainsi que dans différents *fora (Shangri-La dialogue, Manama dialogue, Munich Security Conference…*). Le SGDSN pilote également certains formats particuliers de dialogues bilatéraux (avec l'Australie, l'Inde, Israël, le Japon, le Qatar, le Royaume-Uni ou Singapour, notamment). Il 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.



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

Le SGDSN assure le contrôle des exportations de matériels de guerre et préside à ce titre la Commission interministérielle pour l'étude et l'exportation des matériels de guerre (CIEEMG), qui comprend en outre le ministère des affaires étrangères, le ministère de la défense et le ministère chargé de l'économie. L'exportation de matériels de guerre est interdite sans autorisation. En France, ces autorisations prennent la forme de licences d'exportation, dont l'octroi, après avis de la CIEEMG, relève du Premier ministre, et par délégation du SGDSN. La CIEEMG a instruit 8 200 demandes en 2023. Près de la moitié de ces demandes portent sur des modifications ou des prorogations de licences existantes. Ces chiffres reflètent le maintien à un niveau élevé du nombre des licences délivrées, déjà constaté en 2022 où le cap des 8 000 licences avait été franchi pour la première fois. Une session plénière de la CIEEMG est organisée par le SGDSN chaque mois, afin de débattre des dossiers sensibles ou qui appellent un examen particulièrement approfondi. Le SGDSN est aussi investi dans l'instruction de travaux réglementaires dans ce domaine. S'agissant par exemple des exportations de matériels de guerre dits « intangibles » et dans la continuité de la publication début 2023 du guide qui leur était consacré, un groupe de travail a été constitué pour réfléchir aux moyens de mieux encadrer les nouvelles pratiques numériques et en particulier le travail nomade. En outre, le SGDSN a été particulièrement actif dans la mise en œuvre de 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. Comme en 2022, les acteurs de la CIEEMG ont été particulièrement mobilisés dans le traitement des licences au profit de l'Ukraine. Ces licences, traitées en application du droit commun, ont été examinées prioritairement, dans des délais réduits de 35 % par rapport à la moyenne des licences.

Depuis juin 2023, aux fins de renforcer la cohérence entre les processus de contrôle des exportations sensibles, le SGDSN préside également la commission interministérielle des biens à double usage (CIBDU), qui réunit les ministères concernés et dont le secrétariat est assuré par le service des biens à double usage, qui relève du ministre chargé de l'industrie. A ce titre, le SGDSN contribue au contrôle des exportations de biens et technologies à finalité duale et 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 3 400 demandes de licences individuelles de biens à double usage ont été examinées en 2023. Le SGDSN a participé activement aux travaux d'élaboration, de mise à jour et d'application des sanctions visant la Russie. La dégradation du contexte international renforce le besoin d'un contrôle rigoureux des exportations de ces biens et technologies sensibles.

ÉCONOMIE DE GUERRE

Le 13 juin 2022, le Président de la République a déclaré au salon EUROSATORY que *« nous étions entrés 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 se mobiliser face au retour des conflits de haute intensité, ce qui suppose notamment d'augmenter nos capacités de production.

Pour ce faire, l'accès de la BITD au financement privé est essentiel. Le SGDSN pilote un groupe de travail interministériel consacré à cette problématique, 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 publique 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 en 2023, un séminaire « Banques et industries de défense » afin de renforcer la communication entre ces deux secteurs qui a vocation à se renouveler annuellement. En parallèle, plusieurs initiatives sont en cours pour favoriser les investissements de défense, y compris au niveau européen.

CONTRE-ESPIONNAGE SCIENTIFIQUE, TECHNOLOGIQUE ET SÉCURITÉ ÉCONOMIQUE

Les laboratoires de recherche et entreprises innovantes françaises sont des cibles de choix pour les puissances étrangères, aussi bien lorsque ces dernières cherchent à rattraper leur retard technologique que lorsqu'elles se soucient de conserver leur avance. La prévention des captations et détournements des savoirs, savoir-faire et technologies sensibles à des fins de prolifération d'armes de destruction massive, de renforcement d'arsenaux militaires étrangers, de préparation d'actes de terrorisme ou de guerre économique est une priorité nationale.

Les menaces associées sont quotidiennes, bien que souvent dissimulées. Afin de s'en prémunir, le SGDSN pilote le dispositif de protection du potentiel scientifique et technique de la Nation (PPST) et finalise actuellement des travaux réglementaires visant à le renforcer. Le dispositif de la PPST est pensé pour fournir le juste besoin de protection tout en permettant les échanges académiques ou industriels indispensables à la vitalité de la recherche.

Par ailleurs, le SGDSN préside le comité de liaison en matière de sécurité économique (COLISE), chargé de coordonner l'instruction des décisions proposées au conseil de défense et de sécurité nationale en matière de sécurité économique et le suivi de leur mise en œuvre, et dont le secrétariat est assuré par le commissaire à l'information stratégique et à la sécurité économiques (CISSE). Enfin, le SGDSN participe à l'instruction du contrôle des investissements étrangers en France et est également impliqué dans le suivi des enjeux de défense et de sécurité de plusieurs stratégies nationales technologiques, tels que les technologies quantiques et l'intelligence artificielle.

LES RÉGIMES DE CONTRÔLE AUX EXPORTATIONS

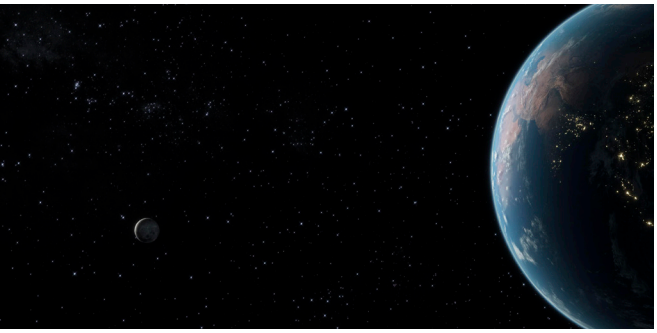
Le SGDSN coordonne la définition de la position interministérielle technique française dans les quatre régimes de contrôles multilatéraux visant à prévenir la dissémination d'équipements et de technologies sensibles : le régime de contrôle de la technologie des missiles (MCTR), l'arrangement de Wassenaar (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, pour les États membres de l'UE, 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 face à de nombreux défis de politisation des échanges et d'instrumentalisation dans le contexte actuel 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 2023 : le travail technique a ainsi permis d'aboutir à l'adoption de nouvelles propositions d'inscriptions aux listes de contrôle (5 au MTCR, 35 à Wassenaar, 5 au groupe des fournisseurs nucléaires, 9 au groupe Australie), dont plusieurs à l'initiative de la France.

PARTICIPER À LA SÉCURITÉ DANS LE DOMAINE SPATIAL



Le bureau des affaires spatiales (BAS) créé en 2022 a été fortement impliqué en 2023 dans la montée en puissance du domaine spatial, que ce soit au niveau de l'UE avec la finalisation du règlement sur la nouvelle constellation connectivité IRIS², les travaux liés à la ministérielle et au sommet de l'ESA, ou encore les problématiques liées à la suspension des lancements de fusées Soyouz depuis le centre spatial guyanais du fait du conflit en Ukraine. Ces travaux nécessitent une forte coordination avec les différents ministères concernés, l'UE et les représentants d'autres États membres. Le BAS assure 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 tant qu'autorité nationale responsable de la sécurité du signal protégé (*public regulated service - PRS*) fourni par le système de radionavigation Galileo, le SGDSN a poursuivi les activités d'instruction des demandes d'autorisation des industriels à travailler sur ce signal. Cette fonction d'autorité nationale responsable est également exercée dans le cadre de la future constellation sécurisée IRIS² et du programme de communications satellitaires européen (Govsatcom).

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 instruire en 2023 les premières demandes des opérateurs concernés par ce champ élargi.

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

IRIS²

Initié en février 2022 pendant la Présidence française du Conseil de l'UE, le programme de l'UE IRIS² vise à assurer d'ici 2028 le lancement d'une constellation pour la fourniture de services gouvernementaux sécurisés de communication par satellite. 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 pour des applications de défense et de sécurité et l'importance de se doter de moyens souverains. Multi-orbitale, cette nouvelle constellation permettra d'entrer dans la course aux méga-constellations en orbite basse dont l'UE est à ce jour absente.

Ce projet s'appuie sur le principe d'un partenariat-public-privé. Un unique consortium constitué des principaux acteurs européens de l'industrie spatiale et des télécommunications, comprenant notamment Airbus, Thales et Eutelsat, travaille depuis mai 2023 sur son architecture. En charge de la sécurité des programmes spatiaux européens, le SGDSN a activement contribué en 2023 à la finalisation du corpus documentaire de l'UE fixant les exigences de sécurité du programme. Jusqu'à la remise de l'offre finale, reportée au 1er trimestre 2024, le SGDSN a ainsi poursuivi cet effort avec un suivi étroit des travaux des industriels et du bon respect de leur part des exigences fixées.

Officiellement nommé le 20 octobre 2023 comme « autorité compétente en matière de connectivité sécurisée » pour la France, le SGDSN continuera à jouer un rôle clé tout au long de la vie du programme : gestion des demandes de services, priorisation et autorisation des utilisateurs nationaux, vérification des équipements… soit autant de missions qui ont impliqué de lancer en fin d'année des travaux interministériels afin de se préparer à assurer ce rôle.

CAROLINE **FERRARI**

Directrice des affaires internationales, stratégiques et technologiques

« La coopération avec nos alliés est plus que jamais nécessaire pour faire front face à l'ensemble des crises que nous traversons. »

Quel rôle joue votre direction dans la coopération avec nos alliés et partenaires sur les questions de sécurité et de défense ?

La coopération avec nos alliés est plus que jamais nécessaire pour faire front face à l'ensemble des crises que nous traversons. L'ensemble des missions d'AIST comporte un volet de coopération internationale : que ce soit en matière d'anticipation stratégique, de suivi et de veille des crises internationales mais également de lutte contre la prolifération des armes de destruction massive, de protection de notre patrimoine scientifique et technologique ou encore de sécurité des programmes spatiaux ou d'exportation des matériels de guerre et de biens à double usage.

Nous échangeons régulièrement avec nos grands partenaires sur l'ensemble de ces questions et intervenons au sein des instances internationales (OTAN, régimes multilatéraux de contrôle, *etc.*) et européennes. Sur le plan bilatéral, les équipes d'AIST concourent, avec l'ensemble des directions et services du SGDSN, au pilotage de grands dialogues stratégiques, porté par le Secrétaire général.

Pour reprendre l'expression de l'historien britannique Adam Tooze, nous sommes entrés dans une ère de « polycrises » (guerre en Ukraine, au Soudan et en Israël, attaques hybrides contre les démocraties, dérèglement climatique et atteintes graves à la biodiversité). Quelle place tient la direction AIST dans l'identification et l'analyse de ces situations de crises ?

L'une des missions de la direction est de participer au suivi et à l'anticipation des évolutions susceptibles d'affecter la défense et la sécurité nationale, ainsi qu'à la préparation de la réponse de l'État dans ce domaine. En complément des travaux d'anticipation interministériels qui se concentrent sur un horizon de 6 à 24 mois, elle est donc, au quotidien, engagée dans une veille attentive des signaux faibles, potentiellement annonciateurs de nouvelles dégradations du contexte géopolitique. Cette fonction est rendue possible grâce aux multiples flux d'informations en provenance des ministères et des services dont bénéficie le SGDSN. La qualité des relations de confiance établies au sein d'un large réseau interministériel d'experts tient également une place essentielle dans ce dispositif.

Alors que 2023 a confirmé notre entrée dans cette ère de polycrises, le rôle interministériel du SGDSN permet à nos autorités de disposer d'une analyse transversale pour établir des liens entre plusieurs phénomènes, qu'ils soient climatique, financier ou géopolitique, et renforcer ainsi nos capacités de réaction et de résilience collectives.

Veiller à garantir notre souveraineté et à protéger nos intérêts fondamentaux est au cœur des missions du SGDSN. Comment la direction AIST y contribue-t-elle ?

C'est une mission essentielle, et la direction y concourt au quotidien, par exemple au travers de notre rôle-pivot en matière de lutte contre les menaces hybrides - qui sous leurs différentes formes (informationnelles, économiques, cyber, mais aussi juridiques avec le *lawfare*) représentent autant d'atteintes potentielles à notre souveraineté. Nous veillons également – à travers le dispositif de protection du potentiel scientifique et technique (PPST) de la Nation mais aussi le contrôle des exportations de biens sensibles – à ce que nos savoir-faire critiques pour notre souveraineté soient protégés, en particulier face au risque de captation ou de prédation de la part d'acteurs hostiles. Dans le même temps, nous portons une attention particulière à la contribution des exportations vers nos partenaires, à la résilience de notre base industrielle et technologique de défense et donc à notre souveraineté capacitaire. En matière spatiale enfin, préserver notre accès souverain à l'espace et doter l'UE d'une capacité autonome pour la fourniture de services spatiaux essentiels au fonctionnement de notre société font partie de nos objectifs prioritaires. Enfin, nous accordons une grande attention aux enjeux de souveraineté associés aux technologies émergentes (intelligence artificielle, technologies quantiques ou biotechnologies) afin de bien structurer la réponse de l'État, que ce soit en actualisant l'état de la menace ou en instruisant des études spécifiques sur ces sujets.

LA CYBERSÉCURITÉ FACE AUX DÉFIS D'ÉVÉNEMENTS D'AMPLEUR

UNE MENACE ÉTATIQUE ET CYBERCRIMINELLE TOUJOURS EN HAUSSE

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) constate en 2023 une augmentation du niveau de la menace informatique, dans un contexte marqué par de nouvelles tensions géopolitiques et l'organisation d'événements internationaux sur le sol français. L'ANSSI estime que les attaquants réputés liés à la Chine, à la Russie et à l'écosystème cybercriminel constituent les trois principales menaces, tant pour les systèmes d'information français les plus « critiques » que pour l'écosystème national dans son ensemble.

Plus particulièrement, l'agence remarque une augmentation significative du ciblage d'entités travaillant dans des domaines stratégiques – groupes de réflexion, instituts de recherche et entreprises de la base industrielle et technologique de défense – ou qui assurent la transmission de données sensibles, comme les entreprises de télécommunications et de fourniture de services numériques (ESN). En parallèle, l'ANSSI constate une augmentation du nombre d'attaques contre des téléphones portables professionnels et personnels afin d'espionner leurs propriétaires. Cette tendance va de pair avec la prolifération de solutions offensives commercialisées par des entreprises privées.

Les attaques informatiques à des fins d'extorsion sont toujours très nombreuses en 2023, avec un regain du nombre d'attaques par rançongiciel contre des organisations françaises. La cybercriminalité représente donc toujours une menace importante pour le secteur public et les entités particulièrement sensibles aux interruptions de service, notamment dans les secteurs de la santé et de l'énergie.

En 2023, l'ANSSI constate également un regain du nombre d'attaques destinées à promouvoir un discours politique, à entraver l'accès à des contenus en ligne ou à porter atteinte à l'image d'une organisation. En France, ces actions de déstabilisation se sont principalement matérialisées sous la forme d'attaques par « déni de service distribué » (DDoS) conduites par des groupes d'hacktivistes pro-russes très réactifs à l'actualité, mais dont les effets restent limités.

L'ANSSI S'IMPLANTE EN BRETAGNE AVEC UNE NOUVELLE ANTENNE À RENNES

Le 22 novembre 2023, l'ANSSI a inauguré sa nouvelle antenne à Rennes. Cette installation, la première hors de l'Ile-de-France, témoigne de la volonté de l'agence de renforcer les synergies avec l'écosystème public et privé déjà implanté à Rennes. Le bassin rennais rassemble en effet un certain nombre de partenaires importants de l'ANSSI, qu'ils soient institutionnels (direction générale de l'armement, ministère de l'intérieur, commandement de la cyberdéfense, direction interministérielle du numérique), académiques et industriels. La capitale bretonne dispose également d'une expertise historique forte dans le domaine de l'informatique et des réseaux et, depuis plus récemment, dans le domaine de la sécurité numérique. L'agence prévoit d'accueillir jusqu'à 200 agents à Rennes à horizon 2025.

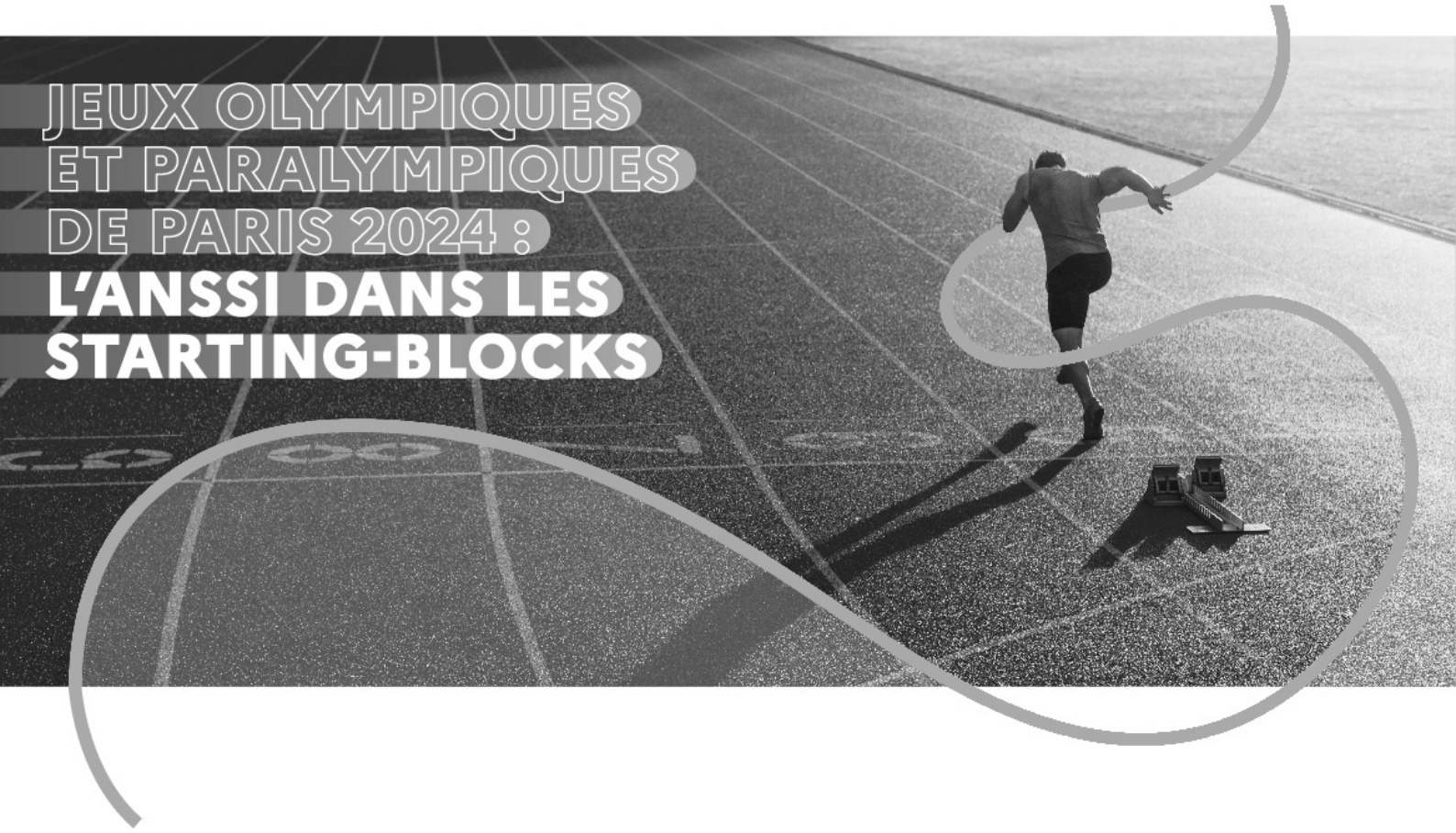
L'ANSSI est désormais présente sur quatre sites distincts : l'Hôtel national des Invalides et la Tour Mercure à Paris, le Campus Cyber à Puteaux et le bâtiment Artefact à Rennes.

LA PRÉPARATION CYBERSÉCURITAIRE DES JEUX OLYMPIQUES ET PARALYMPIQUES

En raison de leur portée médiatique mondiale, les jeux Olympiques et Paralympiques 2024 (JOP) sont susceptibles d'attirer l'attention de divers acteurs cybermalveillants cherchant à profiter de cet événement 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.

Compte tenu de l'ampleur de la menace, la Première ministre a confié à l'ANSSI le pilotage de la stratégie de prévention des cyberattaques des JOP, en juillet 2022. À cette fin, le dispositif mis en place par l'ANSSI, en étroite collaboration avec les différentes structures impliquées dans l'organisation des jeux – dont en particulier la délégation interministérielle aux jeux Olympiques et Paralympiques (DIJOP), le ministère de l'intérieur et des outre-mer (MIOM) et le comité d'organisation des jeux Olympiques et Paralympiques (Paris 2024) – s'articule selon cinq axes principaux :

- parfaire la connaissance des cybermenaces pesant sur les jeux ;
- sécuriser les systèmes d'information « critiques » ;
- protéger les données sensibles ;
- sensibiliser l'écosystème des jeux ;
- se préparer à intervenir en cas de cyberattaque affectant les jeux.



Tout au long de l'année 2023, l'agence a déployé un plan de sensibilisation au bénéfice de plusieurs centaines d'acteurs de l'écosystème des jeux. Elle a mené des actions spécifiques auprès d'une centaine d'acteurs d'une importance particulière pour la préparation et le bon déroulement des jeux, afin de sécuriser leurs systèmes d'information, en particulier au travers d'audits de cybersécurité et d'un accompagnement technique.

Plusieurs exercices de gestion de crise ont également été organisés pour se préparer collectivement à réagir en cas de cyberattaques. En complément, l'ANSSI a aussi mis à disposition un kit d'exercice JOP massifié, spécifiquement conçu pour organiser un exercice simulant le contexte des jeux et ainsi aider les organisations à se préparer à la gestion d'une crise d'origine cybersécuritaire.

CHIFFRES CLÉS

3 703 événements de sécurité

1 112 incidents

15 logiciels publiés en open source

172 qualifications

97 certifications

4 180 demandes de formation CFSSI

269 visas de sécurité délivrés

1 644 personnes formées

57 823 attestations SecNumacadémie délivrées

70 formations labellisées SecNumedu

8 guides techniques publiés

35 formations labellisées SecNumedu-FC

23 articles scientifiques publiés

12 avis techniques publiés

VINCENT **STRUBEL**

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

« Nous devons offrir des réponses adaptées à des menaces qui se sont étendues à l'ensemble de notre société et qui n'épargnent plus personne. »

Quel bilan dressez-vous de votre première année passée à la tête de l'ANSSI ?

Cette année a été marquée par des réalisations notables qui ont fortement mobilisé les agents de l'ANSSI. Elle a également été marquée par une élévation de la menace, en particulier à l'encontre d'acteurs majeurs pour notre sécurité nationale, parmi lesquels des industriels de la défense, des entreprises de télécommunications et des services numériques.

Pour faire face à cette menace, les travaux sur la loi de programmation militaire 2024-2030 ont constitué un travail collectif remarquable et un vrai progrès en dotant l'ANSSI de nouvelles capacités opérationnelles. Les travaux de transposition de la directive *NIS2* ont également été engagés. Nous ne sommes pas au bout du chemin mais nous avons déjà franchi quelques étapes majeures.

Avec la coupe du monde de rugby, nous avons eu l'occasion d'éprouver nos dispositifs opérationnels en vue des jeux Olympiques et Paralympiques de Paris 2024 (JOP). Nous avons aussi évalué notre capacité à mettre en œuvre des procédures d'alerte et d'accompagnement des victimes de cyberattaques efficaces, conjointement avec les autres acteurs de l'État. Il est plus que probable que cette capacité soit mise à l'épreuve à une autre échelle lors des jeux.

La préparation des JOP a également occupé en 2023 et mobilise encore en 2024 un grand nombre d'agents, pour sécuriser, sensibiliser ou préparer à la gestion de crise le vaste écosystème des parties prenantes à l'organisation des jeux. Ce projet nous permet de nous interroger sur le « dépassement capacitaire » et les réponses à apporter en cas d'incidents d'ampleur. Un événement de cette envergure nous oblige donc à penser au-delà des échelles habituelles.

De façon générale, l'accroissement de la menace nécessite également de renforcer nos échanges avec nos partenaires nationaux. L'inauguration en fin d'année de notre antenne rennaise en constitue une illustration. Elle nous apporte d'intéressantes perspectives de coopération avec des partenaires importants au sein des ministères comme la DGA, la direction interministérielle du numérique, le COMCYBER, le ministère de l'intérieur et des outre-mer, mais aussi des interlocuteurs académiques et industriels. Nous voyons déjà le fruit de ce rapprochement avec certains acteurs et j'en suis ▸▸▸

particulièrement ravi.

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

Notre écosystème étant de plus en plus étendu et la menace de plus en plus élevée, l'enjeu majeur est celui de la poursuite du changement d'échelle de notre action et des services que nous offrons, afin de pouvoir toucher un public plus large. Les grands chantiers que nous devrons mener en 2024 s'inscrivent naturellement dans cet objectif.

Nous devons offrir des réponses adaptées à des menaces qui se sont étendues à l'ensemble de notre société et qui n'épargnent plus personne. Les PME, collectivités territoriales ou établissements de santé sont désormais des victimes régulières de cyberattaques, non ciblées, mais de plus en plus industrialisées. Cette menace systémique, apparue ces trois dernières années, est aujourd'hui principalement à motivation lucrative, mais ces modes d'action pourraient très bien être repris par nos adversaires étatiques, dans une logique de sabotage massif. Nous devons donc y répondre, sans perdre pour autant notre capacité à mettre en œuvre des approches très expertes, dans le temps long, pour faire face aux attaques les plus sophistiquées qui ciblent nos administrations et entreprises stratégiques.

Ce défi nous impose d'adapter et d'étendre notre offre de services, mais aussi de développer des coopérations avec un écosystème étendu de partenaires institutionnels, industriels et académiques. L'année 2024 est une année cruciale pour éprouver ces enjeux, avec deux événements majeurs. En premier lieu, les JOP pour lesquels l'ANSSI a été mandatée afin de piloter la stratégie de cybersécurité de l'événement.

L'autre événement majeur c'est bien évidemment la transposition de la directive européenne *NIS2*. Il s'agit d'une directive que nous avons portée lors de la présidence française du Conseil de l'Union européenne. Elle va contribuer à élever le niveau global de sécurité numérique en France en permettant aux entités concernées de mieux se protéger face à une menace devenue systémique. Cette directive induit un élargissement considérable du périmètre des acteurs régulés qui passera de 500 à 15 000 entités en France. Il s'agira pour l'ANSSI d'imposer des mesures proportionnées aux risques auxquels font face ces entités. Cette nouvelle réglementation nécessite une adaptation d'ampleur de l'agence, tant en termes d'organisation que de développement de son offre de services. C'est aussi un défi majeur pour l'écosystème cybersécuritaire qui accompagnera ces entités.

Comment travaillez-vous avec l'écosystème pour amplifier ce mouvement ?

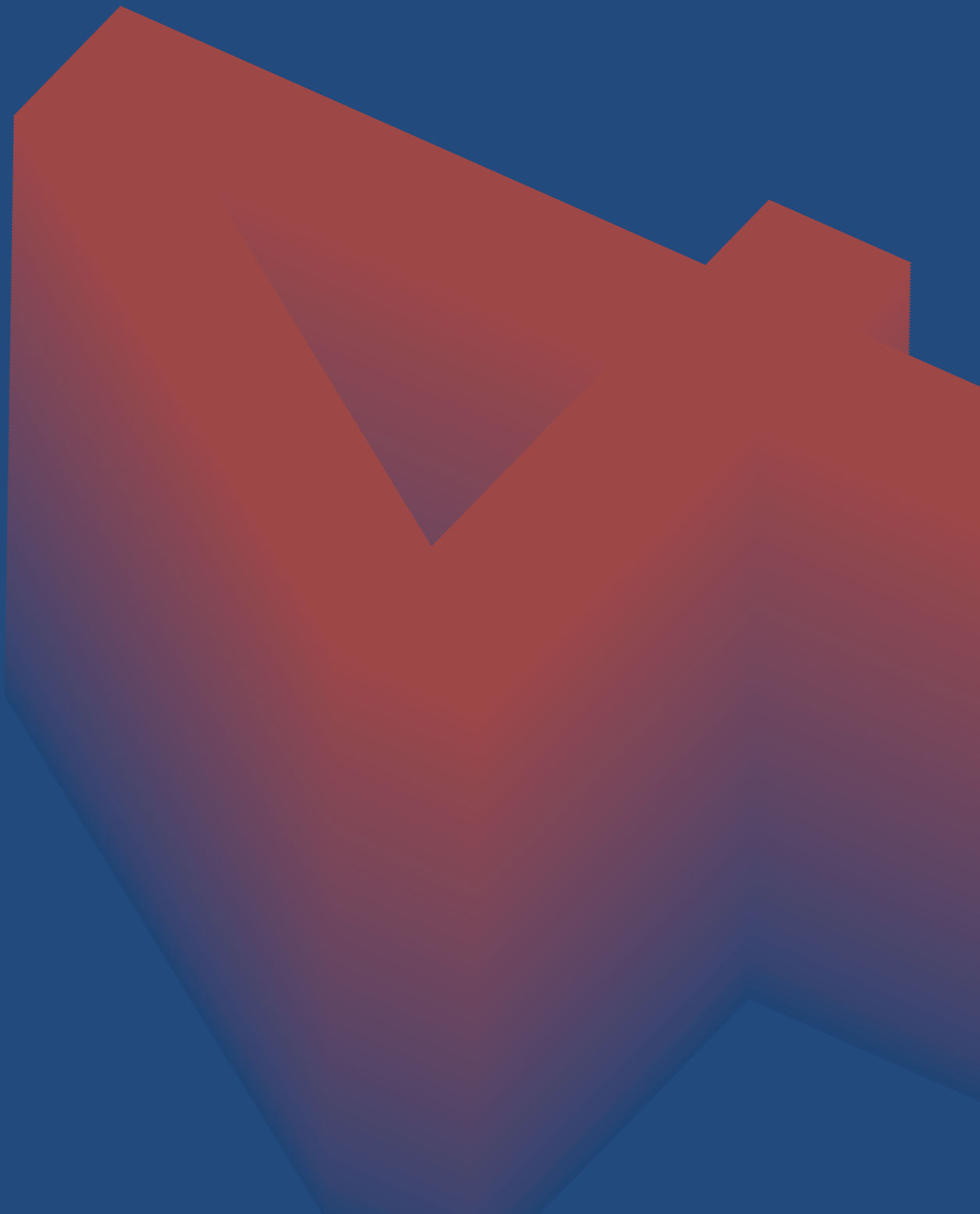
La solution tient en deux idées : maillage territorial et relais de confiance. Je suis profondément convaincu qu'il est nécessaire, pour répondre à la menace à laquelle nous faisons face, de nous appuyer sur des acteurs de confiance et des relais à travers les territoires.

Ce chemin, nous le suivons depuis plus de deux ans, grâce à l'élan donné par le plan France relance. Après avoir accompagné la création de l'association InterCERT France, première association de *CSIRT*, nous accompagnons l'émergence et la structuration de *CSIRT* relais, sectoriels, ministériels ou régionaux, qui participent au renforcement des actions de prévention et d'assistance dans les territoires, au sein des secteurs économiques et de l'administration. Ces *CSIRT* sont devenus des acteurs centraux de la cybersécurité opérationnelle en France. Ce modèle intéresse par ailleurs beaucoup nos partenaires européens.

Le travail en réseau avec l'écosystème doit également se poursuivre et se structurer. Les *CSIRT* relais s'inscrivent en complémentarité avec d'autres dispositifs. Si aujourd'hui nous pouvons nous féliciter d'avoir plus de relais, de points de contact pour les victimes, c'est que collectivement nous avons réussi à étoffer notre écosystème. Ce travail en réseau inclut Cybermalveillance.gouv.fr, les autres acteurs de l'État – police, gendarmerie, justice – ainsi que le Campus Cyber et les prestataires privés.

La prochaine étape, qui est déjà amorcée, vise à structurer et articuler l'ensemble des acteurs existants, ou qui ont émergé récemment. Il est important de nous assurer que la démultiplication de notre action soit faite de manière cohérente et lisible pour ceux qui en ont besoin.◂

LA FIN D'UN CYCLE ET LA PROMESSE D'UN NOUVEAU SOUFFLE



Si l'OSIIC était un athlète, l'année 2023 aurait été l'année de sa préparation à une compétition majeure : à la fois la fin d'un cycle de maturation et l'esquisse d'un nouveau plan d'entraînement pour un jeune organisme atypique et plein de ressources.

Marquée par la nomination du nouveau directeur Yves Verhoeven, l'année fut dense et riche en projets d'envergure, ou en sollicitations multiples, parfois étonnantes, souvent dans l'urgence, toujours au profit des très hautes autorités de l'État et de l'interministériel.

En 2023, l'OSIIC a articulé ses activités autour de trois axes d'efforts : répondre sans délais aux exigences opérationnelles, renforcer la sécurité et la résilience de ses systèmes et adapter son offre de services aux besoins d'utilisateurs aux profils très divers.

RÉPONDRE SANS DÉLAIS AUX EXIGENCES OPÉRATIONNELLES

A l'OSIIC, chaque contexte d'intervention et de déploiement est unique et chaque mission vise à répondre à un enjeu majeur.

Au profit des très hautes autorités de l'État (THAE), la division « opérations » de l'OSIIC a développé une nouvelle solution qui offre la capacité d'échanger des informations classifiées dans des contextes de mobilité toujours plus exigeants. Souple d'emploi, servie par les agents de l'OSIIC, elle a été engagée 8 fois en 2023, année exceptionnelle en nombre de voyages officiels : 30 % de plus qu'en 2022, pour égaler le record de 2015.

L'année 2023 a vu également la généralisation d'une offre de téléphonie mobile sécurisée en réseau fermé développée *ex nihilo* par l'OSIIC, déployée au profit de l'ensemble des membres des cabinets ministériels et de certains directeurs d'administration. Ce projet est une véritable prouesse, à la fois humaine et technique, qui a mobilisé les équipes de l'OSIIC et les services de proximité des cabinets afin d'assurer un déploiement complet à l'été.

L'OSIIC a poursuivi le déploiement des systèmes d'information interministériels classifiés renforçant ainsi son maillage territorial, outre-mer et à l'étranger. Aujourd'hui, plus de 8 000 personnes, sur 650 sites, échangent des informations classifiées en utilisant les systèmes administrés par l'OSIIC. En outre, après l'ouverture d'un premier point d'accès mutualisé interministériel *(hub)* régional à Fort-de-France en 2022, Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale, en a inauguré un deuxième, situé à Marseille, au mois d'avril 2023. Un troisième a été ouvert à Metz quelques mois plus tard. Ces *hubs* offrent la possibilité à tout agent de l'État habilité d'accéder ponctuellement ou lors de ses déplacements à des moyens de communication classifiés.

Lors du déroulement de la coupe du monde de rugby, pendant la phase préparatoire aux jeux Olympiques et Paralympiques de 2024, et bientôt, à l'occasion de la conduite de cet événement majeur, les équipements fournis et administrés par l'OSIIC seront au cœur des échanges interministériels.

RENFORCER LA SÉCURITÉ ET LA RÉSILIENCE DES SYSTÈMES OPÉRÉS PAR L'OSIIC

L'OSIIC a l'obligation d'offrir des services de qualité en permanence face à la menace d'espionnage et doit veiller à maintenir à un haut niveau de sécurité et de résilience les systèmes qu'il opère en vue de protéger les intérêts fondamentaux de la Nation.

L'OSIIC s'est notamment attaché à renforcer la disponibilité et la résilience du réseau de travail « extranet DR » du SGDSN, outil de travail quotidien des agents, devenu progressivement essentiel à la réalisation de leurs missions. Un plan ambitieux a été mis en place dès l'été 2023 afin de disposer, fin 2024, d'un réseau de très haute fiabilité, en migrant progressivement vers une architecture rénovée. Le renforcement des capacités d'hébergement à l'état de l'art au *datacenter* principal de l'OSIIC apporte, dès à présent, une amélioration visible de la disponibilité de ses services.
La mise en place d'un nouveau site d'entreposage au Mont-Valérien, à l'issue d'une manœuvre de déménagement d'ampleur avec le déplacement de plus de 490 palettes en 2 semaines, offre désormais une capacité de stockage accrue, et favorise la disponibilité des équipements sous un préavis très court.

D'autres projets de fond, moins visibles des utilisateurs, ont mobilisé les équipes, notamment la modernisation des réseaux résilients déployés sur la plaque parisienne et directement administrés par l'OSIIC.

L'OSIIC a généré plus d'une dizaine de milliers de certificats, de la carte à puce de connexion à la sécurisation des téléphones portables et des serveurs. La section gestion des éléments secrets (SEGES) assure la comptabilité stricte des articles contrôlés de la sécurité des systèmes d'information (ACSSI) fournis aux ministères et gère aujourd'hui 43 000 articles.

ADAPTER L'OFFRE DE SERVICES AUX BESOINS DE SES UTILISATEURS

L'OSIIC s'est engagé, depuis sa création, dans une démarche de qualité qui passe par l'élaboration d'un corpus procédural complet, couvrant tous les métiers. Cette approche, fondée en partie sur le retour d'expérience, évalue les pratiques et analyse les écarts et les dysfonctionnements, afin de formaliser et améliorer continûment les procédures internes.

C'est une méthode indispensable pour améliorer l'efficacité et l'efficience de l'OSIIC, structurer ses activités et pérenniser ses savoir-faire. *In fine,* cette démarche vise à satisfaire nos bénéficiaires en leur garantissant des services numériques conformes à leurs besoins, aux réglementations et normes en vigueur et à l'état de l'art.

L'année 2023 a, entre autres, été marquée par la construction et la mise en application progressive d'un « processus projet » optimisé, permettant une meilleure implication de nos bénéficiaires tout en garantissant une meilleure fiabilité et une meilleure sécurité de nos services, et permettant, à terme, l'application des méthodes AGILE.

L'OSIIC a poursuivi la refonte et la rationalisation des outils de travail classifiés de l'interministériel et du SGDSN qui offriront, dès 2024, un nouveau visage et de nouvelles fonctionnalités. L'objectif étant de proposer, pour les stations ISIS, un portail modernisé, un bureau numérique rénové et de nouveaux services, tels que le travail collaboratif, la coédition, la visioconférence ou la communication instantanée. D'importants travaux d'adaptation du socle et des infrastructures d'hébergement de nos systèmes ont été réalisés en 2023 pour accueillir ces outils qui vont, sans nul doute, transformer profondément et durablement les usages actuels des systèmes d'information interministériels classifiés. De plus, en offrant un environnement de travail commun aux agents du SGDSN et à l'interministériel, ce chantier améliorera l'efficacité des travaux conjoints et permettra le décommissionnement des réseaux devenus superflus.

En sa qualité de direction numérique du SGDSN, l'OSIIC améliore, de façon continue, son offre de services et anime un réseau de référents au sein du SGDSN afin de recueillir les besoins de chaque direction.

Les agents disposent désormais d'une nouvelle version de téléphone mobile professionnel sélectionné dans le cadre d'un partenariat avec le ministère de l'intérieur : 1 100 terminaux ont été mis en service en trois mois, sur l'ensemble des sites du SGDSN, grâce à une méthode originale saluée par l'ensemble des agents.

Un nouvel espace collaboratif, accessible sur l'extranet et autorisant la coédition d'un document, a fait l'objet de tests avant généralisation en 2024.

Les travaux menés par le bureau « applicatifs » (BAP) de l'OSIIC en 2023 ont permis de concevoir un socle technique commun qui permettra d'augmenter l'agilité dans les projets, d'améliorer la productivité du BAP et de répondre aux demandes croissantes d'hébergement d'applications « métier » par les directions du SGDSN. Par ailleurs, le succès de l'externalisation d'une partie du projet Athéna de gestion des plans de crise de la direction PSE, permet d'envisager de recourir à nouveau à cette organisation pour accroître les capacités de développement de l'OSIIC. Athéna, déjà déployé en version *Bêta*, suit un cycle de développement agile afin d'être disponible en vue des jeux Olympiques et Paralympiques. Trois autres applicatifs métier ont été développés selon la même méthode pour outiller numériquement les politiques publiques du SGDSN et seront livrés pour une première recette fonctionnelle très prochainement.

L'OSIIC a également accompagné l'ANSSI lors de l'installation de son nouveau site à Rennes, ouvert en 2023, et déployé les infrastructures techniques et la desserte des systèmes d'information destinés à 200 utilisateurs à terme.

YVES VERHOEVEN

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

« L'OSIIC est arrivé à la fin d'un premier cycle stratégique et rentre dans une nouvelle phase pour tracer sa voie pour les années à venir. »

Jeux Olympiques et Paralympiques : pouvez-vous nous détailler la façon dont l'OSIIC se prépare à cet événement d'envergure ?

L'OSIIC a pour mission de mettre en œuvre les réseaux classifiées de gestion de crise interministériels et résilients de l'État. Cela implique une posture permanente de préparation et de réaction face à la survenue des crises, qui ne préviennent que rarement avant de se produire.

Durant les JOP, il est essentiel que les systèmes de l'OSIIC soient pleinement fonctionnels afin d'outiller les éventuels besoins de gestion d'incidents à portée interministérielle.

Même si la posture permanente de préparation et de réaction de l'OSIIC pourrait être considérée comme suffisante, la tenue des JOP en France en 2024 justifie qu'un effort encore plus marqué qu'à l'habitude soit réalisé pour faire face à tout aléa survenant pendant la période.

En outre, depuis plus d'un an, l'OSIIC a travaillé avec les ministères et le SGDSN afin d'identifier les besoins supplémentaires d'accès aux réseaux de l'OSIIC et de les déployer bien avant les JOP.

L'OSIIC travaille à l'élaboration d'une nouvelle feuille de route stratégique pour la période 2024-2027. Quelle est l'ambition de l'opérateur ?

Dotée d'un schéma directeur 2020-2023 à sa création, l'OSIIC est arrivé à la fin d'un premier cycle stratégique et rentre dans une nouvelle phase pour tracer sa voie pour les années à venir.
Pour un directeur récemment nommé c'est naturellement une opportunité que de pouvoir lancer rapidement un travail avec son équipe pour définir les grands chantiers qui vont occuper son organisation pour les années à venir, en tirant les leçons de l'expérience des années récentes, et en apportant un regard et un souffle neufs.

Les premiers travaux ont d'ores et déjà fait émerger :

- l'enjeu d'attirer et fidéliser les talents, en les ralliant à notre envie donner le meilleur de nous-mêmes au profit d'une mission qui nous dépasse;
- le besoin d'améliorer notre performance opérationnelle – faire mieux à moindre coût – en travaillant sur notre manière de faire mais aussi en poursuivant la rationalisation et la rénovation de nos systèmes ;
- la volonté de s'inscrire dans les axes de la feuille de route stratégique de la direction interministérielle du numérique (DINUM), en cherchant à outiller numériquement les politiques publiques dont le SGDSN est le garant et en adoptant systématiquement une approche orientée vers l'utilisateur ;
- la pertinence de viser l'excellence en matière de cybersécurité face à une menace de niveau stratégique, en poursuivant le développement de nos capacités tout en bénéficiant de la proximité avec l'ANSSI.

Bien évidemment, cela sera décliné, en lien avec l'ensemble des parties prenantes de l'OSIIC (donneur d'ordres, partenaires, bénéficiaires), permettant ensuite d'aligner l'ensemble des regards vers un horizon partagé, au bénéfice de la protection des intérêts fondamentaux de la Nation.

LUTTER CONTRE LES INGÉRENCES NUMÉRIQUES ÉTRANGÈRES

Le service de vigilance et de protection contre les ingérences numériques étrangères, VIGINUM, est le service opérationnel dont l'État s'est doté depuis 2021 pour renforcer le dispositif national de lutte contre les manipulations de l'information.

VIGINUM a pour mission la protection du débat public numérique et la défense des intérêts fondamentaux de la Nation.

Doté d'une capacité opérationnelle et technique spécifique, VIGINUM se consacre à la détection et à la caractérisation des ingérences numériques étrangères répondant aux quatre critères suivants :

- une atteinte potentielle aux intérêts fondamentaux de la Nation ;
- un contenu manifestement inexact ou trompeur ;
- une diffusion artificielle ou automatisée, massive et délibérée ;
- l'implication directe ou indirecte d'un acteur étranger.

Ses missions sont strictement défensives. Pour les exercer, VIGINUM bénéficie d'un cadre éthique et juridique unique au sein de l'administration, fondé à la fois sur un encadrement réglementaire strict autorisant le service à mettre en œuvre un traitement automatisé de données à caractère personnel, ainsi que sur le travail de son comité éthique et scientifique, placé auprès du secrétaire général de la défense et de la sécurité nationale et qui rapporte annuellement au Premier ministre.

En décembre 2023, VIGINUM a signé une convention de partenariat avec PHAROS, la plateforme de signalement des contenus et comportements illicites sur internet. Ce partenariat accorde à VIGINUM le statut de « signaleur de confiance » auprès de PHAROS.

A quelques mois de l'élection européenne et de la tenue des jeux Olympiques et Paralympiques de Paris 2024, ce partenariat témoigne du renforcement de la coopération entre les services de l'État œuvrant pour la sécurité des citoyens et des visiteurs étrangers.

UNE ACTIVITÉ OPÉRATIONNELLE SOUTENUE FACE À UNE MENACE INFORMATIONNELLE EN EXPANSION

Tout au long de l'année 2023, VIGINUM s'est mobilisé pour détecter, dans le champ informationnel, les tentatives étrangères d'instrumentalisation des différents événements qui ont marqué l'actualité nationale et internationale. Le service a ainsi identifié un volume important de comportements potentiellement « inauthentiques » susceptibles d'affecter le débat public numérique francophone et de nuire aux intérêts fondamentaux de la Nation. Au bilan, VIGINUM a caractérisé près de 13 ingérences numériques étrangères.

230 phénomènes potentiellement inauthentiques détectés

13 opérations d'ingérence numérique étrangère caractérisées

RAPPORT RRN

Depuis le printemps 2022, VIGINUM a identifié une campagne numérique de manipulation de l'information ciblant plusieurs États européens, dont la France et l'Allemagne, ses principales cibles. Baptisée « *RRN* » en raison de la place centrale qu'occupe le « média » Internet *Reliable Recent News* dans cette ingérence, cette campagne poursuit plusieurs objectifs, notamment celui de fragiliser le soutien occidental à l'Ukraine et de grossir le soutien que les populations européennes apporteraient à la Russie.

Particulièrement persistante, cette campagne s'appuie sur plusieurs modes opératoires : la création de réseaux de comptes inauthentiques, principalement sur Facebook et X ; la création de sites web partageant du contenu audiovisuel accusant les dirigeants ukrainiens et les États occidentaux de crimes de guerre ; la création de sites web d'actualité francophones partageant du contenu polémique sur l'actualité nationale française ; l'usurpation de l'identité de médias nationaux et de sites gouvernementaux *via* la technique du *typosquatting*.

De nombreux éléments révèlent l'implication d'individus russes ou russophones ainsi que de sociétés russes dans la réalisation et la conduite de la campagne. VIGINUM a également détecté l'implication d'organismes officiels dans l'amplification de cette campagne. A la suite de l'usurpation de l'identité du site du ministère de l'Europe et des affaires étrangères, la France a décidé de dénoncer cette campagne par le biais de la publication d'un rapport technique recensant les investigations de VIGINUM. Fin juillet 2023, l'Union européenne a adopté des sanctions à l'encontre de 7 individus et 5 entités russes impliqués dans la campagne dévoilée par VIGINUM.

UN COLLECTIF DE TRAVAIL ET UNE ÉQUIPE PLURIDISCIPLINAIRE

En 2023, le recrutement et la structuration du service ont été des enjeux importants. Le service a poursuivi sa croissance d'effectifs et sa montée en compétences, avec 17 recrutements.

A travers la mise en œuvre d'une politique de communication adaptée et la recherche systématique des meilleurs profils, VIGINUM a constitué une équipe rassemblant des savoir-faire rares (OSINT, *data science*, ingénierie informatique, analyse géopolitique) et dotée d'une véritable culture de l'engagement opérationnel.

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

Au cœur du dispositif national de lutte contre les manipulations de l'information, VIGINUM assiste le SGDSN dans ses missions d'animation des travaux de protection et de coordination des différents réseaux interministériels du comité opérationnel de lutte contre les manipulations de l'information (COLMI). Les efforts engagés en 2023 ont permis d'assurer une réponse interministérielle réactive, à l'instar des dénonciations publiques réalisées avec le ministère de l'Europe et des affaires étrangères.

L'action de VIGINUM s'inscrit également dans un environnement international complexe, soumis à la menace représentée par les manipulations de l'information. Ainsi VIGINUM a renforcé ses liens avec plusieurs partenaires étrangers parmi les plus exposés à la menace informationnelle. Les bénéfices de cette coopération sont de plusieurs ordres :

- améliorer la compréhension et la connaissance mutuelles des méthodes et techniques employées par les acteurs de la menace ;
- mettre en commun les réflexions et les approches en matière de résilience de la société;
- conjuguer les efforts pour renforcer la protection des démocraties face aux manœuvres informationnelles.

En 2023, le service a également posé les fondations de sa collaboration avec le monde de la recherche et noué de premiers projets avec des acteurs clés de la communauté scientifique, qu'il approfondira tout au long des années à venir.

RENCONTRES ET DÉBATS AUTOUR DES MANIPULATIONS DE L'INFORMATION

Le 20 juin, VIGINUM a organisé les premières « Rencontres et débats autour des manipulations de l'information », visant à favoriser le dialogue entre les services de l'État et les acteurs du monde de la recherche, œuvrant dans différents domaines : géopolitique, relations internationales, sciences de la donnée, *etc.*

Au programme de cet événement, deux tables rondes : l'une portant sur un panorama de la menace informationnelle ; l'autre sur l'approche pluridisciplinaire de la lutte contre les manipulations de l'information.

La présentation de plusieurs études importantes a apporté un éclairage sur les divers champs de la menace et l'apport possible de la science dans son appréciation.

Fort de ce succès, VIGINUM poursuivra cette démarche d'ouverture, en encourageant la collaboration avec le monde académique, et plus largement la société civile.

MARC-ANTOINE **BRILLANT**

Chef du service de vigilance et de protection contre les ingérences numériques étrangères

« Cet enjeu de résilience de la société sera au cœur des prochaines actions du service. »

Quelle appréciation portez-vous sur la menace informationnelle en 2023 ?

Malheureusement, cette année encore, la France a fait l'objet de nombreuses tentatives d'ingérences numériques étrangères. La guerre en Ukraine et le déclenchement d'un nouveau conflit au Proche-Orient ont servi de prétextes à un grand nombre d'acteurs étrangers pour viser la France de manière désinhibée.

En prenant un peu de recul, il me semble que cette menace informationnelle se caractérise par trois tendances de fond : tout d'abord, ces manœuvres adverses touchent tous les champs du débat public, et plus seulement les élections. Citons en exemple le phénomène des étoiles de David : VIGINUM a pu démontrer qu'un dispositif d'influence étranger avait cherché à amplifier la visibilité des photos sur les réseaux sociaux, dans le but d'attiser les tensions.

Par ailleurs, ces ingérences numériques sont plus élaborées dans leurs modes opératoires qu'auparavant. À ce titre, l'utilisation croissante de l'intelligence artificielle générative est un sujet de préoccupation. Je pense également à la vaste campagne « RRN » révélée en juin dernier. Cette campagne mettait en avant le procédé de l'usurpation d'identité de sites web de médias français et d'institutions officielles pour y diffuser des messages non seulement inexacts mais surtout trompeurs.

Enfin, les acteurs étrangers de la menace recherchent davantage de furtivité en recourant à la sous-traitance, l'usage d'intermédiaires et de relais. Je pense à la campagne que nous avons baptisée « OLIMPIYA » au cours de laquelle nous avons pu démontrer l'action d'une société de communication numérique dont le rôle consistait notamment à dénigrer la capacité de la France à organiser les jeux Olympiques et Paralympiques de Paris 2024 dans de bonnes conditions de sécurité.

Quels enseignements en tirez-vous ?

Si je m'appuie sur les trois tendances de fond que j'évoquais, la menace informationnelle va nous occuper encore longtemps. Les acteurs malveillants paraissent plus nombreux et plus déterminés à perturber la sincérité de notre débat public pour atteindre nos intérêts fondamentaux.

Toutefois, en matière de défense, il me semble que le dispositif interministériel national de lutte contre les manipulations de l'information coordonné par le SGDSN a gagné en efficacité, signe d'une maturité croissante. L'exposition des campagnes « RRN » et « OLIMPIYA » ainsi que notre réactivité collective sur la tentative d'ingérence liée aux étoiles de David en sont d'excellents exemples. Cette efficacité accrue est principalement liée à la relation de confiance qui s'est nouée au fil des opérations avec le ministère de l'Europe et des affaires étrangères, le ministère des armées et le ministère de l'intérieur et de l'outre-mer.

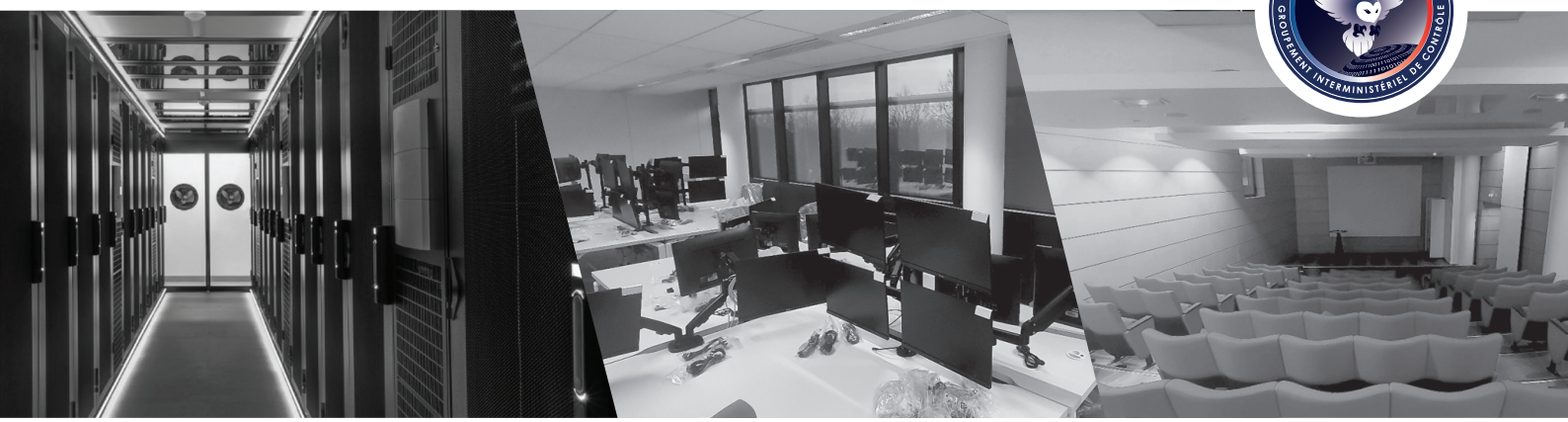
Quels sont les défis pour 2024 ?

L'année 2024 est jalonnée d'événements majeurs, qu'ils soient de nature sportive (JOP24) ou politique (élection européenne du 9 juin), qui sont autant de rendez-vous propices à des manœuvres informationnelles contre la France. En parfaite coordination avec ses nombreux partenaires, VIGINUM s'est préparé pour répondre aux défis associés à la protection du débat public numérique lié à ces événements.

Par ailleurs, de nombreuses zones de tensions et crises internationales subsistent, imposant au service de maintenir une vigilance de chaque instant.

Enfin, l'ensemble des agents du service auront à cœur de renforcer les liens avec le monde éducatif ainsi qu'avec la société civile. Une réponse n'est efficace que si elle est durable et partagée. Aussi, l'année 2024 verra VIGINUM créer et renforcer ses partenariats pour mieux sensibiliser le public, notamment les plus jeunes. Cet enjeu de résilience de la société sera au cœur des prochaines actions du service.

SOUTENIR LE RENSEIGNEMENT



UNE ACTIVITÉ OPÉRATIONNELLE INTENSE

Service opérationnel chargé de centraliser les techniques de renseignement, le groupement interministériel de contrôle a connu un surcroît d'activité en 2023. Le nombre global d'autorisations de techniques de renseignement et le nombre de transcriptions soumises à son contrôle ont crû de 6 %. Même si ce taux est très inférieur à celui des années 2016-2020, il est suffisamment important pour démentir l'impression d'atteinte d'un plateau. L'activité opérationnelle du GIC a été en effet affectée par plusieurs événements, notamment les violences collectives survenues au printemps, les attentats du 13 octobre et du 2 décembre et par la poursuite d'actions souterraines d'ingérence ou d'espionnage, des cyberattaques visibles ou invisibles, dans un contexte international particulièrement dangereux.

Malgré l'opacification des communications électroniques, l'interception de sécurité reste un moyen d'enquête essentiel. Cette technique a été particulièrement sollicitée en 2023, approchant le nombre maximal fixé par le Premier ministre à deux reprises. Dès 2015, le législateur avait introduit et encadré la technique du recueil de données informatiques afin de répondre à la difficulté rencontrée par les interceptions de sécurité qui se heurtent au chiffrement fort du web en général et des messageries sécurisées en particulier. En 2023, le nombre d'autorisations de recueils de données informatiques a logiquement été plus élevé (5,5 %) que celui, contingenté, des interceptions de sécurité (2 %).

Responsable exclusif de l'exécution des algorithmes de détection de menace terroriste (article L. 851-3 du code de la sécurité intérieure), le GIC a mobilisé ses équipes pour optimiser les algorithmes en vigueur et en développer de nouveaux. Le nombre d'alertes a été multiplié par trois.

9 000 objets dans le parc informatique

1 500 agents des services formés à l'utilisation des applications du GIC

73 recrutements

86 sites informatiques

380 autorisations de techniques de renseignement par jour

AU SERVICE DES SERVICES

En 2023 encore, le GIC s'est résolument placé au service des services, à la fois en faisant évoluer les systèmes d'information qu'il leur offre, en améliorant l'accueil de leurs exploitants dans ses locaux et en développant de façon significative la formation, à leur profit, sur les outils qu'il met à leur disposition. Trois fois plus de personnes ont été formées à l'emploi des outils informatiques du GIC grâce à la mise en place d'une équipe de formateurs capable de se projeter sur l'ensemble du territoire national.

Le GIC a amélioré l'ergonomie de ses logiciels et a profondément modifié leur architecture pour qu'ils puissent s'échanger des données, notamment les identifications des objectifs ou de leurs correspondants. Afin de répondre à une demande des autorités de contrôle, il a modifié ses outils de traitement des demandes de techniques de renseignement afin que les géolocalisations en temps réel portent non pas sur un identifiant mais sur une personne, quels que soient ses identifiants, comme le permet la loi. Cette modification aura pour conséquence de réduire le nombre d'autorisations prononcées au titre de l'article L. 851-4 du code de la sécurité intérieure, pour le même nombre d'identifiants électroniques suivis.

L'année 2023 a été marquée par de nombreux travaux de rénovation entrepris dans six centres d'exploitation distants du GIC, au profit des services, et par le début de la construction d'un nouveau point d'interception des communications internationales.

À l'approche des jeux Olympiques et Paralympiques de 2024, le GIC a fiabilisé ses systèmes et réseaux, en remplaçant des équipements fragiles et en intervenant de façon préventive sur ses infrastructures afin de réduire le risque d'une panne survenant entre les mois d'avril et octobre 2024. Ces opérations ont été conduites parallèlement à l'effort de long terme, initié en 2022, de rationalisation des architectures informatiques. Cet effort vise à accroître la fiabilité, la sécurité et à permettre le partage de données entre des applications aujourd'hui étanches entre elles. À terme, l'administration des systèmes sera facilitée et il en résultera une économie de ressources humaines particulièrement rares.

Avec le soutien du SGDSN, le GIC a consommé la totalité de son budget 2023 en fonds normaux et a gréé l'ensemble de ses postes. Par ailleurs, dans l'emploi de ses fonds spéciaux, il s'est conformé aux recommandations de la Commission de vérification des fonds spéciaux qui lui avait déjà accordé un satisfecit pour sa gestion 2022.

UNE CENTRALISATION RÉAFFIRMÉE INCARNÉE PAR UN NOUVEAU SITE

Avec près de 300 agents répartis sur plusieurs sites, accueillant des milliers d'exploitants des services, permanents ou vacataires, le GIC a passé en revue les risques afférents à chacun des postes de travail et a établi une liste de mesures de prévention pour les réduire. Cet effort particulier de prévention a notamment donné lieu à une campagne de formation à la détection et à la prévention des risques psycho-sociaux pour tous les cadres du GIC. Par ailleurs, afin de maintenir un climat de travail sain entre ses différents bureaux dans un contexte marqué par l'éloignement, l'éclatement des équipes et le télétravail, le GIC a organisé plusieurs actions de cohésion, qui contribuent à la qualité des rapports professionnels et de la vie au travail.

En 2024, les priorités du GIC sont, une fois encore, marquées par la poursuite de la centralisation :

- d'abord la centralisation dans l'espace, avec le rassemblement dans un nouveau bâtiment de la sous-direction technique et des sections d'exploitation parisiennes des services, actuellement réparties entre trois implantations ;
- l'exécution centralisée des algorithmes avec la poursuite des développements et la migration vers un nouveau centre de données, l'un des centres actuels étant au bord de la saturation. Le GIC contribuera en 2024 au rapport qui sera présenté au Parlement sur les algorithmes pour la prévention du terrorisme ;
- le démarrage d'un ambitieux programme interministériel de centralisation des recueils de données informatiques, conduit par le GIC, dans la continuité de ses initiatives déjà lancées début 2023.

Avec sa position singulière de tiers de confiance, entre les gisements de renseignement et les services de renseignement, le GIC est d'une part un acteur opérationnel inséré dans la chaîne de recueil et d'exploitation, qui rend compte au Premier ministre et assure la traçabilité de l'emploi des techniques de renseignement. D'autre part, le GIC offre à l'autorité indépendante, la Commission nationale de contrôle des techniques de renseignement, un regard synoptique sur le processus d'autorisation et de mise en œuvre des techniques de renseignement.

MODERNISER LA FONCTION SOUTIEN

Le service de l'administration générale (SAG), service à vocation transversale du SGDSN, anime et coordonne l'ensemble des missions d'administration générale nécessaires à l'activité du Secrétariat général et des services à compétence nationale qui lui sont rattachés, ainsi que celles du groupement interministériel de contrôle. Le service, qui est organisé en deux sous-directions (ressources humaines ; administration générale et finances) et un détachement de gendarmerie, emploie une centaine d'agents de statuts divers.

LES RESSOURCES HUMAINES

L'axe d'effort majeur de l'année 2023 a été le déploiement de RenoiRH, système d'information des ressources humaines, effectué en deux temps : premièrement, le module de gestion administrative début 2023 ; puis le module de paie, après plusieurs mois de longs préparatifs visant à migrer le système, fiabiliser les données et tester l'ensemble. Ce nouveau système d'information a fortement modifié les modes de travail, en faisant émerger la fonction de gestion administrative-payeur et en imposant la réorganisation de la division de la gestion des ressources humaines.

La fonction recrutement a elle aussi été fortement mobilisée. Confrontée à une hausse du schéma d'emploi du SGDSN et à des vacances d'emplois, elle s'est réorganisée. Les ressources humaines de proximité sont désormais plus fortement impliquées : elles sont notamment en charge de la réalisation du dossier de proposition salariale. Cette évolution de la fonction recrutement a permis d'importants gains de temps dans le recrutement des agents du SGDSN. En 2023, 388 recrutements ont été effectués au SGDSN.

Le bureau de gestion du personnel militaire a été mobilisé par la mise en place des différentes primes liées à la nouvelle politique de rémunération des militaires. Le bureau a par ailleurs complètement refondu le circuit de notation des officiers et posé les règles encadrant la télé-activité des militaires.

L'année 2023 aura également été marquée par la rénovation du dialogue social, avec la tenue des premiers comités sociaux d'administration du SGDSN, et de la formation spécialisée en santé, sécurité et conditions de travail. Le nombre de représentants du personnel est ainsi passé de 4 à 11, et les réunions des instances de dialogue social jalonnent désormais l'activité et la transformation du SGDSN.

La promotion des politiques publiques du Gouvernement aura également animé les travaux, avec notamment l'organisation du séminaire ministériel des services de la Première ministre consacré à l'intégration des travailleurs en situation de handicap le 21 novembre ou la préparation de la convention de partenariat signée par la secrétaire générale du Gouvernement le 21 septembre avec l'association La Cordée, chargée de promouvoir la diversité dans l'accès à l'emploi.

La fonction sécurité-sûreté, intégrée organiquement à la sous-direction des ressources humaines, a été consolidée en 2023 par l'arrivée de l'officier de sécurité des systèmes d'information et de la chargée de mission « règlement général sur la protection des données ».
Le détachement de gendarmerie a poursuivi ses missions de protection/sécurisation avec un élargissement sur de nouveaux sites (Rennes, Mont-Valérien, Campus Cyber).

L'ADMINISTRATION GÉNÉRALE ET LES FINANCES

L'année 2023 a été constructive et disruptive.

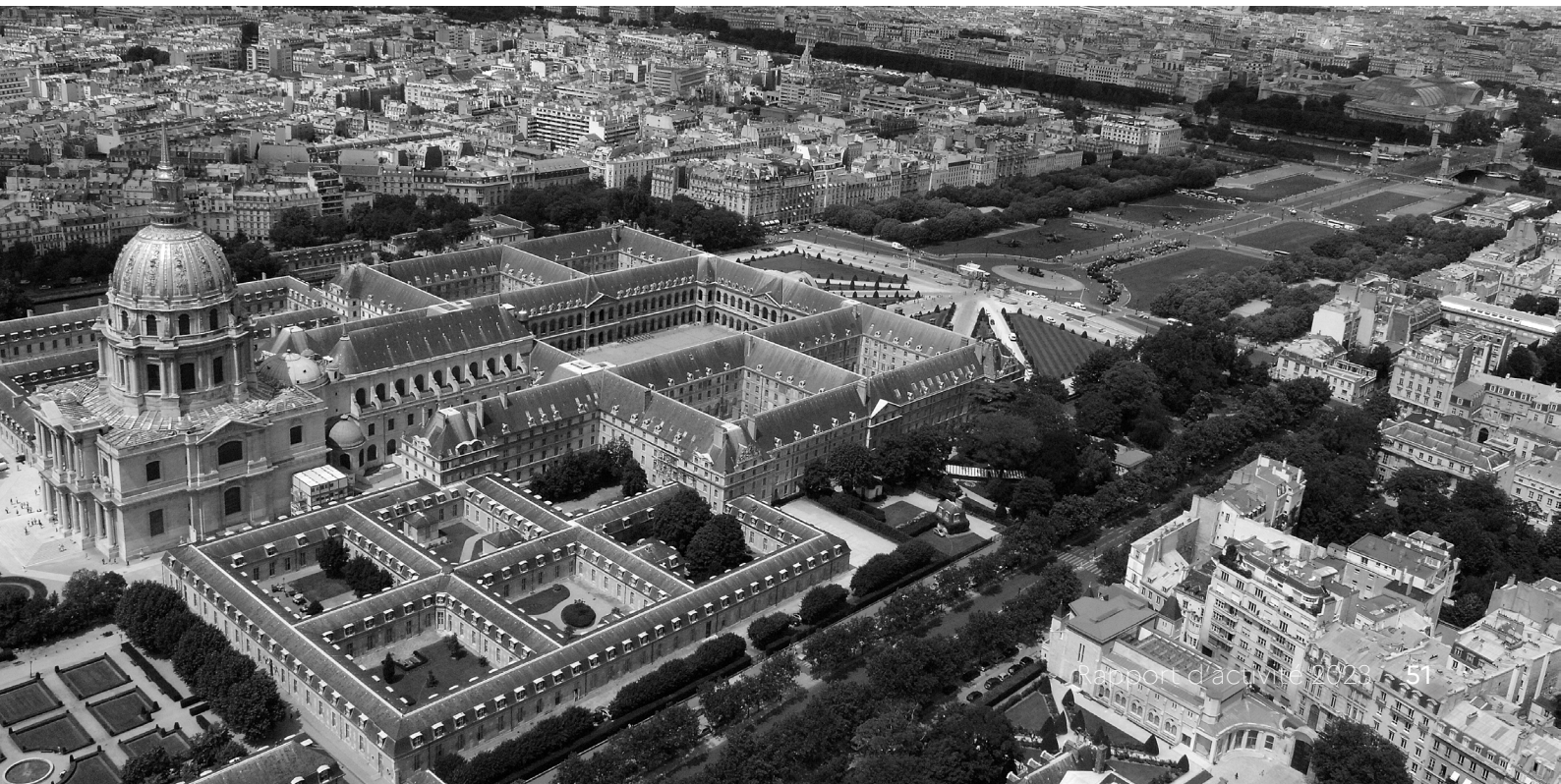
Constructive à travers le renforcement de l'expertise et de la capacité d'ingénierie technique et administrative de la sous-direction au profit du soutien opérationnel de l'ensemble des directions et services du SGDSN. Tous les domaines d'activité de la sous-direction auront été concernés et animés par cette ambition.

Ainsi, l'accompagnement à la livraison et à l'installation des équipes au sein du nouveau bâtiment Artefact à Rennes, qui aura nécessité de croiser vision financière, infrastructure et commande publique ; la mise en œuvre d'un vaste plan de fiabilisation des installations critiques ; la livraison d'un nouveau bâtiment, entièrement réhabilité et réaménagé, au Mont-Valérien ; le pilotage renforcé de la programmation budgétaire qui aura permis une fin de gestion nominale et la préparation de la refonte de l'architecture budgétaire du SGDSN ; l'accompagnement contractuel de la montée en puissance du dispositif de cybersécurisation des sites JOP24 avec 120 prestations intellectuelles commandées ; la préparation du rattachement administratif et financier du Haut-commissaire à l'énergie atomique au SGDSN, ne sont que quelques illustrations marquantes de ce panorama de l'année 2023.

Disruptive également car nombreux sont les chantiers de fond qui ont été initiés avec le souci de « préparer l'avenir » : révision du circuit d'exécution de la dépense et de la régie ; refonte du processus de traitement des missions ; établissement d'un schéma d'occupation des locaux prélude à la définition d'une stratégie immobilière pluriannuelle ; définition d'une politique d'archivage ; lancement du changement de système d'information pour la gestion documentaire ; mise en place, à fin d'expérimentation, de Chorus formulaire au sein du bureau logistique ; ces chantiers de la feuille de route ont animé et continuent d'animer la SDAGFIN.

En 2024, SAG travaille sur d'importants dossiers de fond.
Sans être exhaustif, peuvent être cités :

- une feuille de route « Transition écologique » ;
- un schéma pluriannuel de stratégie immobilière et la poursuite des grands chantiers infra ;
- RENOIRH décisionnel ;
- le développement de l'offre de formation ;
- la protection santé/prévoyance et le renouvellement du marché de la médecine de prévention ;
- l'engagement dans la démarche de la labellisation égalité professionnelle hommes/femmes ainsi que diversité/handicap ;
- l'accompagnement des JOP qui vont immanquablement impacter nos missions.



CHIFFRES CLÉS

1 188,18 **emplois travaillés** (prise en compte du temps de présence et de la quotité de travail) constatés au 31/12/2023

388 recrutements

Dialogue social

5 comités sociaux administratifs

2 formations spécialisées santé, sécurité et conditions de travail organisés

+ 98 ETP

39 000 **jours** de télétravail indemnisés

99,4 % taux d'atteinte du schéma d'emplois au 31/12/2023

213 M€ de budget

5 800 demandes de paiement (**+ 11 %** par rapport à 2022)

40 marchés publics lancés (**+ 18 %** par rapport à 2022)

8 974 **articles** sélectionnés par le bureau documentation pour la réalisation de la revue de presse et des veilles particulières

5 600 ordres de mission traités (**+ 25 %** par rapport à 2022)

3 000 bons commande notifiés (**+ 28 %** par rapport à 2022)

1,4 **millions de tirages** réalisés par l'atelier impression

314 opérations logistiques (**+ 39 %** par rapport à 2022)

9 **mètres linéaires** d'archives transférés au service historique de la défense

LINE BONMARTEL-COULOUME

Cheffe du service de l'administration générale

« Le SGDSN s'est engagé en 2023 dans les travaux préparatoires à l'accord-cadre ministériel sur l'égalité entre les femmes et les hommes »

Comment se traduit l'engagement du SGDSN dans la politique interministérielle de promotion de l'égalité entre les femmes et les hommes ?

Le SGDSN est particulièrement attentif à l'égalité de traitement entre ses agents et la fonction « ressources humaines » est en première ligne pour promouvoir l'égalité femmes/hommes au travers de mesures concrètes.

Ainsi, la campagne 2023 de rebasage des salaires (« primes structurelles ») s'est appuyée sur un nouveau critère d'égalité salariale femmes/hommes, venu compléter les critères antérieurs (promotion, mobilité fonctionnelle, clause de revoyure triennale) pour déterminer le montant des primes à allouer.

En matière d'accès aux responsabilités pour les emplois de direction, dans le cadre de la politique de nominations équilibrées, le SGDSN a nommé 5 femmes sur des emplois de directrices d'administration centrale, de cheffe de service et de sous-directrices, atteignant ainsi en une année l'objectif qui lui était fixé pour l'horizon 2027.

Au-delà de ces emplois de direction et au profit de l'ensemble de ses agents, le SGDSN s'est engagé en 2023 dans les travaux préparatoires à l'accord-cadre ministériel sur l'égalité entre les femmes et les hommes, qui a été signé par la secrétaire générale du Gouvernement le 8 mars dernier, journée internationale des droits des femmes. Cet accord, fruit d'une concertation avec les organisations syndicales des services du Premier ministre, va permettre de renforcer les actions en faveur de l'égalité entre les femmes et les hommes, comme par exemple le recours à un guide du recrutement permettant de recruter sans discriminer, l'amélioration de la formation en matière de culture de l'égalité, la poursuite des efforts pour réduire les écarts de rémunération et le renforcement de l'offre d'action sociale aux aidants et à la parentalité.

Quels sont les enjeux immobiliers du SGDSN à moyen et long terme ?

Le SGDSN est actuellement implanté sur 7 emprises immobilières dont 4 domaniales (Hôtel national des Invalides, Montrouge, Rennes, Mont-Valérien) et 3 locatives (Tour-Mercure, Le Ponant, Campus Cyber).
Cette empreinte immobilière doit aujourd'hui répondre à trois enjeux.

Le premier enjeu est celui de la cohérence de la stratégie immobilière. Il s'agit d'un poste de dépenses élevé : 8,8 M€ de loyer en 2024. Il importe d'anticiper des besoins pérennes. Il faut, aussi, décliner les orientations gouvernementales en matière de politique immobilière de l'État, comme l'objectif interministériel de réduction de la surface de bureau louée ou détenue à l'horizon 2027, et de transition écologique, comme la cible interministérielle de réduction de la consommation énergétique des bâtiments tertiaires de 25 % et de réduction des surfaces de 7,5 % à l'horizon 2027.

Le deuxième enjeu est celui de l'adaptation des ressources immobilières aux besoins fonctionnels et techniques des directions et services en veillant à diminuer les vulnérabilités techniques, à garantir la cohérence du positionnement des services et à assurer la qualité de vie au travail.

Troisième enjeu, en lien avec les deux précédents, celui de la capacité à absorber de manière cohérente la poursuite de la croissance des effectifs du SGDSN sur la période 2024-2027, soit 200 ETP supplémentaires arbitrés à ce stade.

Pour accompagner cette évolution, différents chantiers, dont la rénovation et l'affectation de bâtiments sur le site du HNI ont été lancés. Le GIC de son côté rationalise son empreinte immobilière en Ile-de-France autour de deux emprises.

Si l'année 2023 a permis de réaliser un état des lieux actualisé de l'occupation d'une partie des locaux du SGDSN, la préparation de l'avenir rend désormais nécessaire l'établissement d'un schéma pluriannuel de stratégie immobilière. Articulé autour d'un diagnostic technique préalable et d'une analyse fonctionnelle, il doit permettre d'apporter des réponses à ces enjeux dès 2024.

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