PREMIER
MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Rapport d'activité 2019– 2020

Rapport d'activité 2019–2020

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 :
Cercle studio

Coordination éditoriale :
Justine Boquet

Sommaire

Édito

Stéphane Bouillon
Secrétaire général de la défense et de la sécurité nationale

Quels que soient l'époque et les évènements, le secrétariat général de la défense et de la sécurité nationale – SGDSN – se doit d'être aux rendez-vous que lui fixent le Président de la République et le Premier ministre. J'ai souhaité que soit publié ce rapport d'activité qui couvrira 2019 et 2020 pour en rendre publiquement compte. Le lecteur y verra qu'en dépit de circonstances exceptionnelles – je pense notamment à la pandémie – aucune mission n'a été interrompue.

Pendant 18 de ces 24 mois, la responsabilité de secrétaire générale aura été assurée par Claire Landais, nommée secrétaire générale du Gouvernement le 15 juillet 2020. Ce rapport est donc autant un hommage à la marque qu'elle a imprimée sur le SGDSN, tant à l'interne qu'à l'interministériel, qu'à l'investissement permanent et sans faille des 1 279 agents qui servent au sein de cette maison aux nombreuses missions.

Moins qu'un document de présentation exhaustif, ce rapport est un *compendium*, un résumé. Il vient donner un coup de projecteur sur le vaste domaine de la défense et de la sécurité nationale, envisagé d'un point de vue tout à fait particulier : celui des acteurs de la concertation interministérielle.

Rarement en charge de la mise en œuvre des politiques menées sur le terrain – il existe quelques exceptions – le SGDSN est avant tout un facilitateur, un négociateur et un promoteur. Sa fonction est d'abord et avant tout de présenter à ses autorités les solutions dégagées en commun avec les ministères, visant à anticiper, promouvoir, prévenir ou remédier. Cette fonction se matérialise tout particulièrement dans le rôle de secrétariat du Conseil de défense et de sécurité nationale, qui a pris une importance toute particulière depuis 2015. Cette instance très régulièrement réunie par le Président de la République a considérablement étendu le champ de ses sujets d'intérêt et la temporalité des politiques qu'elle supervise, compte tenu de l'intrication accrue des enjeux de défense et de sécurité et de sécurité nationale à l'extérieur et à l'intérieur de notre pays.

Pour cette raison, le SGDSN a dû lui aussi élargir la palette de ses travaux. Il a dû évoluer et se transformer, notamment en mettant en œuvre son plan stratégique 2019-2022. En cela, il est fidèle à une tradition aussi vieille que lui : depuis 1906, le SGDSN évolue, se transforme, change au gré des choix de ses chefs, de leurs priorités et des grands bouleversements historiques. Cette plasticité est la marque d'une volonté de tous ses agents de toujours mieux servir, aujourd'hui et demain.

Je vous souhaite une bonne lecture. ◄

Entretien avec le secrétaire général

Les années 2019 – 2020 ont été marquées par une crise sanitaire majeure. Quelles en ont été les répercussions sur l'activité du SGDSN ?

De par son positionnement, au service du Premier ministre et dans le champ de la défense et de la sécurité nationale, le SGDSN a évidemment été concerné par la réponse à la crise sanitaire qui touche notre pays. Plus spécifiquement, le SGDSN travaille sur la préparation et la planification des réponses à apporter aux crises, dont les crises sanitaires. Dans la crise de la Covid-19, il a appuyé le Premier ministre et les ministères « menants », sur les aspects non sanitaires. D'ores et déjà, des leçons pour l'avenir ont été tirées et une grande réforme de la planification de sécurité est en cours, principalement en vue de simplifier nos grands plans.

Naturellement, la crise sanitaire a également eu des effets sur le fonctionnement du SGDSN. Nos agents ont dû être placés en télétravail, alors que ce type d'aménagement était assez peu pratiqué antérieurement. Je tiens d'ailleurs à saluer le professionnalisme sans faille dont ils ont fait preuve. Je dois aussi saluer la remarquable performance de l'OSIIC qui a produit des outils nomades adaptés dans des délais extraordinaires. Au bilan, nous avons parfaitement assuré la continuité de nos missions.

Comment le SGDSN se met-il en ordre de bataille pour tirer les enseignements de la pandémie et se préparer à de nouvelles crises de portée similaire ?

Depuis le printemps 2020, à la suite du premier confinement, le SGDSN tire les enseignements de la crise afin de renforcer la préparation du pays et améliorer la réponse aux crises futures. Le SGDSN a ainsi été mandaté par le Premier ministre pour conduire une réflexion interministérielle en vue d'élaborer une stratégie nationale de résilience. Celle-ci pourrait prévoir de diffuser plus largement la culture de l'anticipation, de généraliser les plans de continuité d'activité, de développer une approche territoriale de la gestion de crise et de refondre la planification. Pour y aider, le SGDSN élabore une nouvelle version du guide de réalisation d'un plan de continuité d'activité et a entamé la refonte des plans de gestion de crise. Nous espérons faire aboutir notre réflexion en 2023 et 2024.

►►►

▶▶▶

En 2019 et en 2020 le SGDSN a conduit des transformations internes. Comment l'institution évolue-t-elle ?

Claire Landais, ma prédécesseure, a doté le SGDSN d'un plan stratégique pour la période 2019-2022. Plusieurs chantiers ont été conduits durant cette période, avec pour objectif d'améliorer ou d'adapter l'organisation interne et de renouveler les méthodes.

Deux de ces chantiers ont été particulièrement structurants. Le premier porte sur la transformation numérique du SGDSN, afin de répondre aux enjeux de numérisation et de doter le SGDSN d'un écosystème moderne en la matière, tout en prenant en compte les contraintes de sécurité propres à notre activité. La création de l'opérateur des systèmes d'information interministériels classifiés (OSIIC) et le fait de lui confier la direction des systèmes d'information du SGDSN marquent cette volonté d'entrer dans une nouvelle ère numérique.

Le second chantier porte sur la transformation du SGDSN dans le domaine de la politique des ressources humaines. De par les profils spécifiques qu'il recrute, mais également en raison des flux importants de départs et d'arrivées, le secrétariat général de la défense et de la sécurité nationale se devait de revoir son approche des ressources humaines. Plusieurs projets sont menés, dont l'objectif commun est de contribuer à la satisfaction de besoins croissants de recrutement, de diversification et de spécialisation.

De nouvelles menaces apparaissent, d'autres se concrétisent (menaces hybrides, haute intensité, cyberattaques, champ informationnel…). Comment le SGDSN se prépare-t-il à accompagner l'État face à ces défis ?

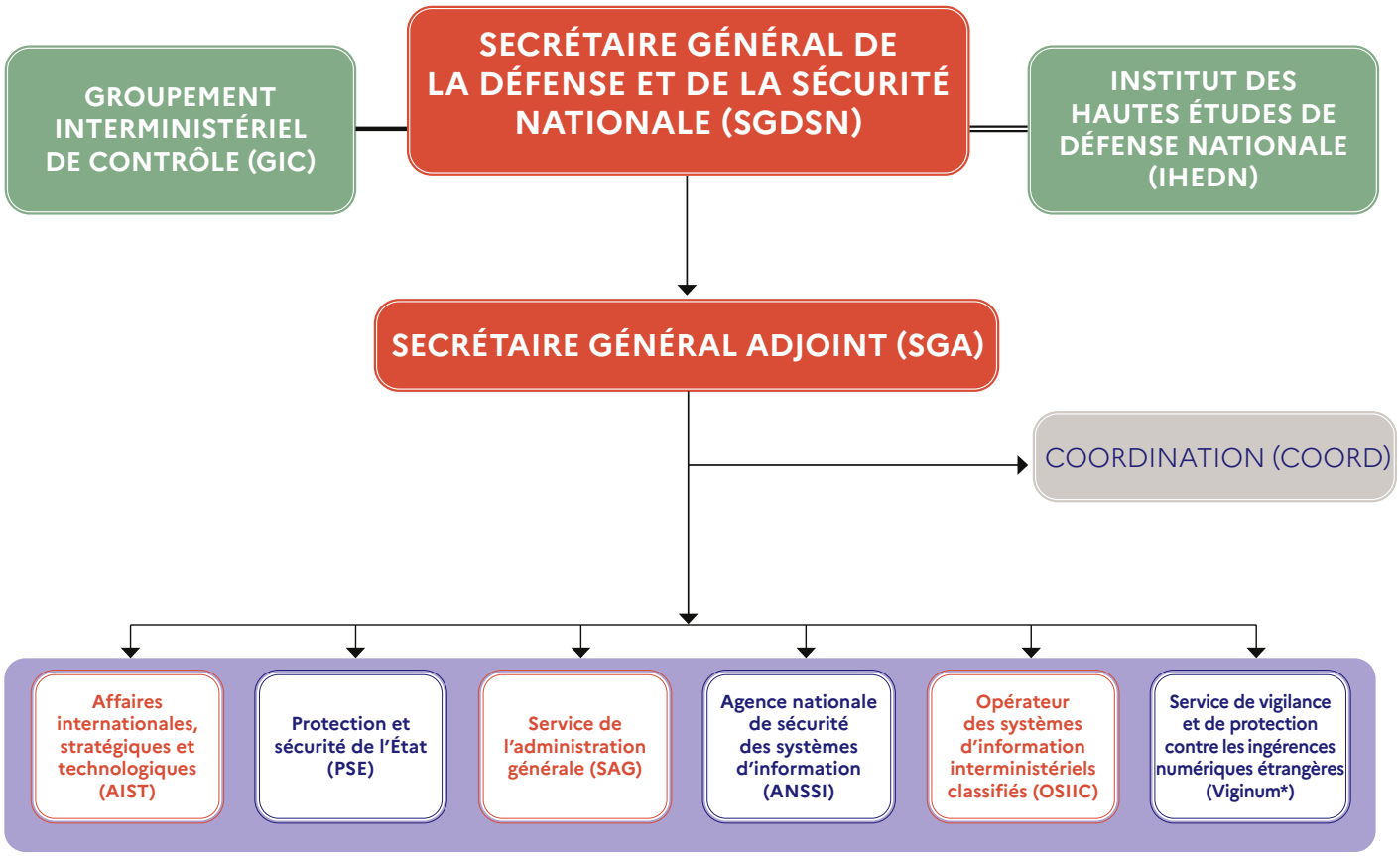
Disposer d'une approche prospective dans la conduite de nos missions est absolument indispensable. L'ANSSI démontre depuis de nombreuses années sa réactivité, sa capacité à travailler avec les autres services et sa performance face aux attaques cyber dans le privé comme dans le public. Nous sommes autant la maison de l'anticipation que de la gestion de crise. Nous sommes en outre organisés pour animer des travaux d'anticipation. Dans un passé récent, des travaux ont été conduits sur les ruptures technologiques, sur l'environnement stratégique de la France à l'horizon 2030. Un travail est en cours avec le ministère de l'Europe et des affaires étrangères sur l'avenir de certaines zones géographiques et sur des sujets stratégiques. Une doctrine française visant à répondre aux menaces hybrides a par ailleurs vu le jour et elle doit s'articuler avec la stratégique européenne en cours.

Parmi ces travaux d'anticipation, on peut également citer la concertation interministérielle sur la lutte contre les manipulations de l'information, ayant – entre autres – abouti à la création d'un nouveau service à compétence nationale, rattaché au SGDSN, le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum).

Les mois à venir doivent nous permettre de réfléchir à un constat préoccupant : l'instrumentalisation du droit et des normes par certains pays, afin d'asseoir leur domination pour défendre leurs intérêts derrière de grands principes. Face à ces nouveaux enjeux, face au bouleversement des équilibres géopolitiques et économiques, le SGDSN continuera à améliorer ses méthodes de travail pour répondre aux orientations fixées en Conseil de défense et de sécurité nationale. ◀

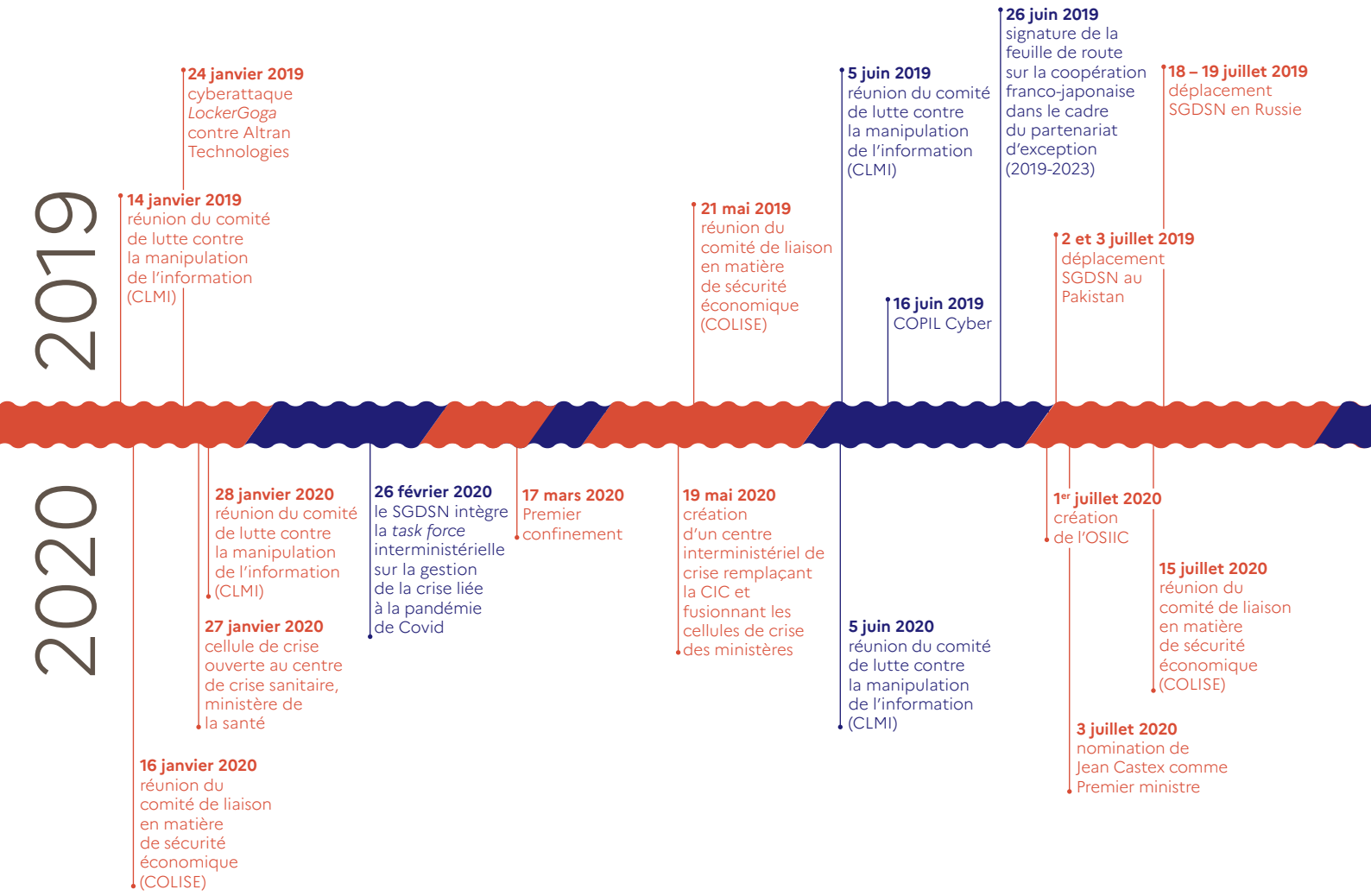
Organigramme

en date du 10 septembre 2021



* Service à compétence nationale créé par décret du 13 juillet 2021

Chronologie 2019– 2020



LA CELLULE INTERMINISTÉRIELLE DE CRISE :

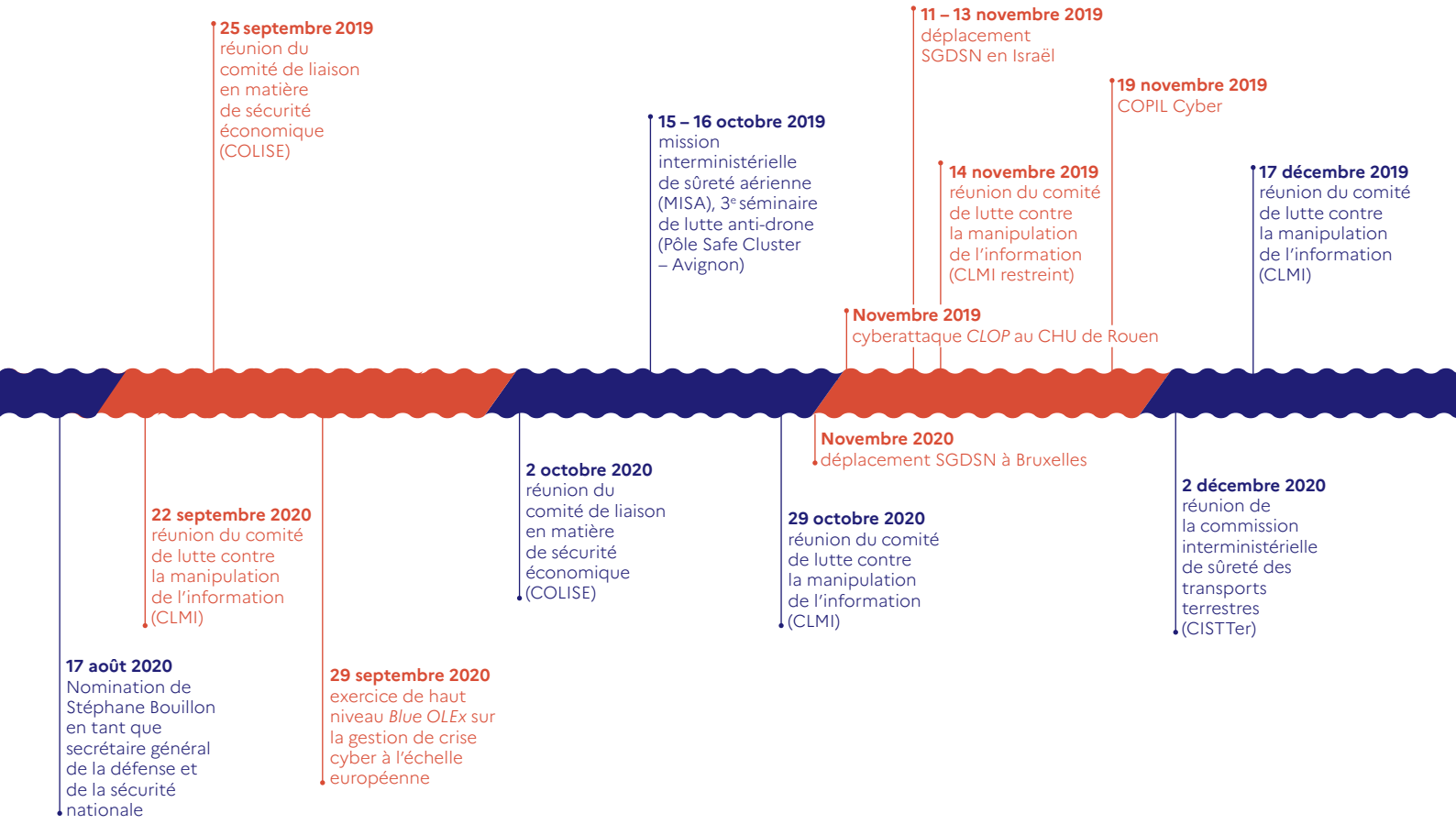
17 mars 2020
activation de la CIC Covid

25 septembre 2020
attentats dans les anciens locaux de *Charlie Hebdo* – activation de la CIC

16 octobre 2020
assassinat de Samuel Paty à Conflans Saint Honorine – activation de la CIC

29 octobre 2020
attentat au couteau devant la basilique Notre-Dame de Nice – activation de la CIC

29 octobre 2020
attentat au consulat général de France à Djeddah – activation de la CIC



CISA

La commission interministérielle de sécurité aérienne s'est réunie à trois reprises sur la période 2019 – 2020
12 juin 2019, 10 décembre 2019 et 16 décembre 2020

EVOLUTION DE LA POSTURE VIGIPIRATE AU COURS DE LA PÉRIODE 2019 – 2020

7 mai 2019 : posture Vigipirate été – automne 2019 niveau *sécurité renforcée – risque attentat*

19 octobre 2019 : posture Vigipirate automne – hiver 2019 niveau *sécurité renforcée – risque attentat*

5 mai 2020 : prolongation de la posture Vigipirate automne – hiver 2019 – printemps 2020 niveau *sécurité renforcée – risque attentat*

26 octobre 2020 : posture Vigipirate automne – hiver 2020 – printemps 2021 niveau *sécurité renforcée – risque attentat*

30 octobre 2020 adaptation de la posture Vigipirate au niveau *urgence attentat* suite à l'attentat de Nice

LE SGDSN, UNE STRUCTURE OPÉRATIONNELLE TOURNÉE VERS L'INTERMINISTÉRIEL

Anticiper, prévenir et instruire

La stratégie Indopacifique de la France

Suite à la présentation, en mai 2018, par le Président de la République, de la vision française pour l'Indopacifique, et de la stratégie de défense pour l'Indopacifique du ministère des armées, rendue publique en 2019, le SGDSN a été missionné pour copiloter, avec le ministère de l'Europe et des affaires étrangères, les travaux de mise en œuvre de ces positions. Cela s'est notamment traduit par le développement de la dimension interministérielle ainsi que l'identification d'objectifs stratégiques et d'actions concrètes dans quatre domaines :

- la sécurité et la défense ;
- l'économie, la connectivité ; la recherche et l'innovation ;
- le multilatéralisme et le droit ;
- la lutte contre le changement climatique, la protection de la biodiversité et la gestion durable des océans. ◄

Rafale indien

Menaces hybrides

Matérialisant une crispation notable dans les relations internationales, les menaces hybrides sont devenues une préoccupation centrale pour les pays européens. Les modes d'action hybrides sont caractérisés par la combinaison d'actions directes et indirectes, jouant avec les différents seuils de réaction et visant à obtenir des gains, tout en évitant le conflit armé interétatique.

En France, la capacité à répondre à des menaces hybrides repose sur la coordination interministérielle. Celle-ci doit garantir la mobilisation rapide des leviers pertinents de l'État pour traiter les menaces hybrides dirigées contre la nation. Afin de poursuivre cet objectif, le SGDSN pilote un groupe de travail interministériel permanent sur les menaces hybrides. Il prend, par ailleurs, une part active aux réflexions conduites au sein du Centre d'excellence européen sur les menaces hybrides d'Helsinki. Le SGDSN participe enfin à l'élaboration des positions nationales au sein du groupe *Enhancing Resilience and Countering Hybrid Threats* de l'Union européenne.

Dialogues stratégiques

Le SGDSN anime ou contribue à certains dialogues bilatéraux de sécurité dans la zone indopacifique. Il entretient par exemple des contacts réguliers avec Singapour sur des thématiques variées. Enfin, dans le cadre du partenariat d'exception entretenu avec le Japon, le SGDSN pilote le dialogue global sur l'espace, concentrant les axes de coopération civile et militaire.

Anticipation

Le SGDSN a piloté au cours de l'année 2019-2020 des travaux interministériels d'anticipation d'envergure. Ils ont porté sur des sujets géographiques (influences étrangères dans les Balkans, mer Rouge, enjeux énergétiques en Méditerranée orientale, Mozambique, etc.) et thématiques (perspectives d'évolution de l'ingérence numérique étrangère à des fins de manipulation de l'information).

Contrôler les exportations de matériels sensibles

Le SGDSN assure un rôle moteur dans le contrôle des exportations de matériels de guerre (EMG) et contribue au contrôle des exportations de biens à double usage (BDU) :

▶ Les matériels de guerre : le SGDSN assure le contrôle des exportations de matériels de guerre au travers de la commission interministérielle pour l'étude et l'exportation des matériels de guerre (CIEEMG). Les matériels de guerre étant soumis à un régime de prohibition, leur exportation est interdite sans autorisations spécifiques. En France, elles prennent la forme de licences d'exportation, dont l'octroi, sur avis de la CIEEMG, relève du Premier ministre.

La CIEEMG a instruit 7 300 demandes de licences d'EMG en 2019 et 8 000 demandes en 2020. La moitié de ces demandes porte sur des modifications ou des prorogations de licences existantes. Cet accroissement des demandes de prorogation en 2020 s'explique par le contexte de crise sanitaire qui a freiné les démarches commerciales et la recherche de nouveaux marchés.

Le SGDSN anime également des travaux interministériels et internationaux relatifs à l'élaboration ou à la modification de politiques d'exportation de matériels de guerre. Le SGDSN est ainsi impliqué dans l'instruction de travaux réglementaires dans ce domaine.

▶ Les biens à double usage : le SGDSN a par ailleurs contribué à l'instruction des dossiers les plus sensibles soumis à la commission interministérielle des biens à double usage (CIBDU) parmi les quelques 5 000 demandes de licences reçues annuellement par le Service des biens à double usage de Bercy. Il a enfin participé aux travaux de refonte du règlement européen (CE) 428/2009 instituant un régime de contrôle des exportations de biens à double usage, lesquels ont conduit à l'adoption du règlement (UE) 2021/821 entré en vigueur le 9 septembre 2021.

▶ En 2020, la mission d'information parlementaire sur le contrôle des exportations d'armement, menée par les députés Jacques Maire et Michèle Tabarot, mentionnait le rôle majeur que jouent les EMG pour l'équilibre et la pérennité de la base industrielle et technologique de défense (BITD) française, ainsi que pour le maintien de notre autonomie stratégique en lien avec la politique étrangère de la France. Le domaine des exportations des BDU était également abordé.

Les propositions émises dans ce rapport ont conduit à l'adoption de mesures que le Premier ministre, les ministres concernés et le secrétaire général de la défense et la sécurité nationale ont présentées aux parlementaires en juin 2021. Elles portent principalement sur trois domaines : une réforme du fonctionnement de la CIBDU, un alignement du processus d'arbitrage des autorisations d'exportation des BDU sur celui des EMG, et le renforcement de l'information au Parlement avec la publication à partir de 2022 d'un rapport annuel sur l'exportation des BDU, à l'instar de celui existant sur les EMG. Le Premier ministre a également approuvé un nouveau décret qui formalisera la présentation périodique devant le Parlement, par les ministres des armées, de l'Europe et des affaires étrangères et de l'économie, des finances et de la relance, des résultats en matière d'exportation d'armements et de BDU. ▶▶▶

L'Accord franco-allemand sur les exportations d'armement

Signé le 23 octobre 2019, cet accord permet de fluidifier les échanges entre les industries de défense française et allemande, notamment de composants destinés à être intégrés dans un système d'arme, puis réexportés. Cet accord définit des principes d'autorisation d'exportations selon trois cas d'usage, dès lors que l'opération envisagée ne « porte pas atteinte à la sécurité nationale ou aux intérêts directs » des partenaires :

- ▶ les coopérations intergouvernementales (article 1) ;
- ▶ les coopérations industrielles (article 2) ;
- ▶ les produits destinés à être intégrés dans un système d'arme, développés en dehors du cadre des coopérations intergouvernementales et industrielles (article 3).

Pour les cas où les articles 1 et 2 ne s'appliqueraient pas, l'article 3 prévoit l'application du principe dit « *de minimis* » : la valeur des composants transférés doit rester en deçà du seuil de 20 % de la valeur totale du produit final et ces composants ne doivent pas être considérés comme sensibles. Plus d'une centaine d'opérations d'exportation ont été autorisées par les autorités françaises et allemandes au titre de l'article 3 de l'accord. ◀

▶▶▶

Lutter contre la prolifération des armes de destruction massive et contrôler la diffusion des technologies et savoir-faire sensibles

Le SGDSN anime la politique de lutte contre la prolifération et la dissémination des biens et technologies sensibles.

En premier lieu, il assure une veille permanente dans les domaines concernés, notamment dans les domaines nucléaire, biologique, chimique, des explosifs, des missiles et du spatial, et il coordonne les positions techniques de la France dans les différents « régimes » multilatéraux de contrôle des exportations qui visent à définir les transferts sensibles méritant d'être contrôlés : Arrangement de Wassenaar (armes conventionnelles et biens et technologies à double usage), Régime de contrôle de la technologie des missiles (*MTCR* en anglais), Groupe de l'Australie (armes chimiques et biologiques) et Groupe des fournisseurs nucléaires (*NSG* en anglais).

En second lieu, il pilote le dispositif interministériel de protection du potentiel scientifique et technique (PPST). Celui-ci vise à prévenir les tentatives de captation de savoirs et savoir-faire stratégiques par des puissances étrangères, des prédateurs technologiques ou économiques, ainsi que leur détournement à des fins de prolifération (armement conventionnel ou de destruction massive) ou de terrorisme. La PPST est fondée sur la constitution de « zones à régime restrictif » (ZRR) au sein des établissements publics de recherche ou des entreprises. L'accès à ces ZRR est contrôlé. À travers un dialogue étroit entre les services spécialisés de l'État et les acteurs de la recherche publique ou privée, cette réglementation concilie liberté de la recherche, dynamique des relations économiques et besoins de protection. Le nombre de ZRR s'est accru de 8 % en 2020, ce qui témoigne de l'intérêt porté au dispositif par les acteurs privés et publics.

Enfin, le SGDSN assure un rôle de coordination de l'ensemble des administrations mobilisées dans le cadre de la mise en œuvre des actions d'entrave aux trafics de biens et technologies proliférantes.

COLISE

Sous l'impulsion du Président de la République, qui a souhaité une réforme de la politique publique de sécurité économique, un comité de liaison en matière de sécurité économique (COLISE) réunit régulièrement depuis septembre 2018 des représentants des huit principaux ministères concourant à cette politique. Présidée par le secrétaire général de la défense et de la sécurité nationale, cette instance de coordination a notamment permis d'élaborer un référentiel interministériel unique identifiant des entreprises et des technologies essentielles, ce qui facilite le suivi des menaces pesant sur nos intérêts économiques. ◀

Covid-19 : contrôle à l'exportation des équipements de protection individuelle

En 2020, la crise sanitaire de la Covid-19 s'est accompagnée d'une très forte tension mondiale sur les équipements de protection, notamment les masques. Dans ce contexte, l'Union européenne a voulu contrôler les exportations de ces équipements afin de répondre aux besoins urgents et vitaux sur son territoire et limiter les exportations aux seuls besoins légitimes (actions humanitaires, etc.).

En lien avec les ministères en charge de l'économie et de la santé, le SGDSN a ainsi contribué à la mise en œuvre des règlements (UE) 2020/402 du 13 mars 2020 puis (UE) 2020/568 soumettant à autorisation l'exportation de certains équipements de protection individuels (EPI) contre la Covid-19.

Dans le cadre de ce dispositif, les autorités françaises ont examiné près de 700 demandes d'exportation déposées par 136 exportateurs. Sur l'ensemble de ces demandes, 92 refus ont été prononcés pour 1,4 million d'équipements.

Participer à la sécurité des programmes spatiaux européens

L'Union européenne conduit actuellement plusieurs programmes majeurs dans le domaine spatial : Galileo et Egnos pour le positionnement par satellites, Copernicus pour l'observation de la terre, GovSatCom pour la fourniture de capacités et de services de télécommunications au profit d'infrastructures critiques et enfin SSA relatif à la surveillance de l'espace. La maîtrise de la sécurité des programmes spatiaux européens exige d'entretenir une relation de proximité avec les autres administrations nationales, la Commission européenne et les États qui participent à ces programmes, qu'ils soient européens ou non. Du fait du caractère transversal de ce sujet, la synthèse des positions nationales sur la sécurité est assurée par le SGDSN.

En 2019 et 2020, les travaux ont été principalement axés sur la négociation du nouveau règlement « espace » de l'UE qui vise à unifier le cadre juridique des programmes spatiaux majeurs de l'UE afin d'en clarifier la gouvernance et d'en améliorer la sécurité tout en facilitant leur accès aux industriels européens et en particulier aux PME. Par ailleurs, la définition des capacités de la seconde génération des systèmes de positionnement par satellites Galileo a permis la signature, début 2021, du premier contrat pour le renouvellement des satellites.

Concernant Galileo, le SGDSN, qui exerce les fonctions d'autorité nationale responsable de la sécurité du signal protégé (*Public regulated service*), a continué, en 2019 et en 2020, d'accompagner le déploiement de ce système, qui devrait être totalement opérationnel en 2024.

Satellite IOV Galileo

Contrôler l'imagerie spatiale de haute résolution

Dans le domaine spatial, le SGDSN assure le contrôle de la diffusion des images d'origine spatiale par les opérateurs industriels. Le processus a été simplifié en 2020 avec la suppression de la commission interministérielle des données d'origine spatiale (CIDOS), dont les membres sont désormais consultés informellement. Le SGDSN est également étroitement associé aux évolutions de la régulation des activités spatiales comme par exemple le *Space Traffic Management*. ◄

3 questions à...

Jean-Hugues Simon-Michel

Directeur des affaires internationales, stratégiques et technologiques (AIST)

Quels enjeux stratégiques identifiez-vous sur les années 2019-2020, susceptibles d'être structurants à moyen terme ?

Sans conteste, le renouveau des menaces hybrides. Les deux dernières années ont marqué un renforcement de la compétition globale des acteurs étatiques et non étatiques, où tout conflit est désormais empreint d'hybridité. Depuis 2019, le concept de menaces hybrides connaît un renouveau dans les réflexions de l'Organisation du traité de l'Atlantique Nord et de l'Union européenne. L'UE a ainsi adopté un cadre conceptuel sur les menaces hybrides en 2020, identifiant treize champs d'actions prioritaires.

Parmi ceux-ci, la France en a retenu cinq sur lesquels elle souhaite porter ses efforts : cybernétique, lutte contre la manipulation de l'information, l'utilisation de l'arme normative (*lawfare*), sécurité économique et champ opérationnel.

Quel regard portez-vous sur le processus de contrôle des exportations de matériel de guerre (dites EMG) que votre direction anime ?

Les mécanismes de la commission interministérielle pour l'étude et l'exportation des matériels de guerre sont robustes. La CIEEMG procède à un examen approfondi de chaque demande de licence d'export au travers notamment des huit critères de la position commune européenne de 2008. Pour autant, j'identifie deux axes d'effort : la recherche d'une plus grande cohérence entre le régime de contrôle des exportations de matériels de guerre et celui des biens à double usage et le soutien à l'exécutif pour assurer une information renforcée du Parlement sur nos politiques d'exportation de matériel de guerre.

Quelles sont les réponses apportées par l'État pour protéger les savoirs et savoir-faire tout en préservant la liberté de la recherche ?

Voulu comme un espace de dialogue privilégié entre, notamment, les acteurs de la recherche et l'administration, le dispositif interministériel de protection du potentiel scientifique et technique de la Nation (PPST), piloté par le SGDSN, repose sur l'adhésion volontaire de ces acteurs, qu'ils soient publics ou privés. En dépit d'actions de sensibilisation et malgré l'action croissante de puissances étrangères sur le territoire national, la prise de conscience de la communauté scientifique sur ces enjeux tarde, dans un contexte de compétition technologique pourtant exacerbée au niveau international. Les administrations concernées ont donc engagé des travaux interministériels visant à renforcer les moyens de lutte contre la captation ou la divulgation non contrôlée de savoirs et savoir-faire sensibles.

Planifier pour renforcer

Renforcer la gestion des crises

Le SGDSN a conduit une série d'exercices sur la période 2019-2020 destinés à renforcer la capacité de l'État à gérer les crises. Conduit en janvier 2019, l'exercice PIRATAIR 18 a permis d'éprouver la préparation face aux attaques terroristes dans le secteur aérien. En novembre 2019, le SGDSN a également conduit un exercice de réaction face aux crises sanitaires de grande ampleur et mis à l'épreuve le nouveau plan national de lutte contre la variole lors de l'exercice VARIOLE 19.

La période 2019-2020 a également été marquée par la révision et la signature au 1er juillet 2019 de la circulaire du 2 janvier 2012 relative à l'organisation gouvernementale pour la gestion des crises majeures, ainsi que par l'adoption d'une nouvelle instruction interministérielle portant organisation de la cellule interministérielle d'information du public et d'aide aux victimes (C2IPAV). En parallèle de ces travaux de planification, un programme ambitieux de formation des acteurs de la gestion de crise (PAGC) a été inauguré au mois de mars.

Opération Sentinelle 2020, dispositif renforcé suite à l'adaptation de la posture VIGIPIRATE au niveau *urgence attentat*.

Lutter contre le terrorisme

Le SGDSN a suivi la mise en œuvre du plan d'action contre le terrorisme (PACT) présenté par le Premier ministre le 13 juillet 2018. Après plusieurs mois de travaux interministériels intenses, le SGDSN a diffusé en octobre 2019 un guide de mise en œuvre des dispositions législatives relatives à la détection et au traitement des agents contractuels publics, fonctionnaires et militaires, exerçant des missions en lien avec la souveraineté, la sécurité ou la défense, dont le comportement deviendrait incompatible avec ces fonctions.

L'année 2019 a été particulièrement marquée par la tenue du sommet du G7 en France, à Biarritz, les 25 et 26 août. Le SGDSN a participé à la préparation de cet événement, travaillant sur plusieurs mois à l'adaptation de la posture VIGIPIRATE, à l'anticipation de différents *scenarii*, et à l'animation de deux exercices locaux d'entraînement à la veille du sommet en liaison avec le ministère de l'Europe et des affaires étrangères et le ministère de l'intérieur.

L'anticipation de la menace terroriste sur la période 2019-2020 s'est accompagnée d'un important effort de sensibilisation. Mise en ligne en septembre 2019, la plateforme VIGIPIRATE « *faire face ensemble* » a été conçue pour acculturer le grand public, les personnes en charge de la sécurité des ERP (établissements recevant du public) et les élus locaux à la menace terroriste et appréhender les gestes et réflexes à adopter en cas d'attaque. Le site totalisait plus de 12 000 personnes inscrites à la fin de l'année 2019.

Enfin, la mise en place d'une certification des équipes cynotechniques pour la recherche d'explosifs et la création du centre national d'évaluation des performances des chiens à Biscarosse ont fait l'objet d'une validation interministérielle lors de la commission interministérielle de sûreté des transports terrestres (CISTTer) du 3 décembre 2019.

Développer des technologies de sécurité

Le SGDSN a réalisé en octobre 2019 une démonstration de solutions de lutte anti-drones à Avignon et a organisé dans un grand port la mise en œuvre opérationnelle d'une expérimentation grandeur nature de lutte contre le trafic illicite de matière nucléaire et radiologique.

Le SGDSN a également pu expérimenter des technologies de sécurité dans la perspective des Jeux olympiques et paralympiques de 2024 qui se tiendront à Paris. Après le lancement de plusieurs appels à manifestations d'intérêts qui ont permis de labelliser 135 solutions technologiques, le SGDSN a réalisé des expérimentations en situation réelle au cours du tournoi de Roland-Garros en septembre 2020. Ces travaux ont permis de tester des technologies de gestion de flux de personnes ; de détection de comportement anormal ; de dématérialisation et de sécurisation de billets ; de contrôle d'accès biométrique ou encore de détection d'intrusions.

Protéger les informations classifiées

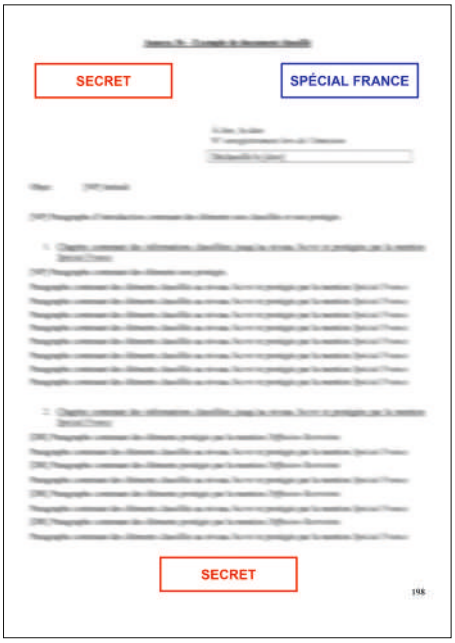
La publication du décret n° 2019-1271 du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale a permis de poursuivre la préparation de la réforme dont l'entrée en vigueur a eu lieu en 2021.

Les consultations interministérielles ont ainsi permis de refondre l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, approuvée par arrêté du 13 novembre 2020. Cette nouvelle instruction clarifie les règles relatives au maniement des informations et supports classifiés dans un contexte de dématérialisation accélérée. Elle tire les conséquences du besoin d'échange accru avec les acteurs privés et les partenaires étrangers, en alignant les standards de protection sur les standards internationaux, pour faciliter les échanges tout en garantissant le niveau de sécurité.

Parallèlement à son volet règlementaire, la réforme comprend un plan de modernisation des outils de pilotage de la protection du secret et de son suivi ministériel et interministériel, le renforcement de l'offre de formation et l'élaboration de guides pratiques à destination des « praticiens » du secret de la défense nationale.

Afin d'accompagner les acteurs dans la mise en œuvre de cette importante réforme, le SGDSN a développé des outils et des supports pédagogiques : des fascicules de sensibilisation à la protection du secret et à sa réforme, une formation en ligne opérationnelle depuis janvier 2018 et une formation à la protection du secret.

Sur le plan européen, la négociation des aspects liés à la protection des informations classifiées des programmes de l'Union européenne pour la période 2021-2027 (programme Horizon Europe, programme spatial de l'Union européenne…) a constitué un point d'intérêt majeur. L'année 2020 a également été marquée par la poursuite des travaux d'élaboration et de refonte des cadres règlementaires des institutions européennes pour la protection de leurs informations classifiées, qui s'intensifieront au cours de l'année 2021. ▶▶▶



Avec le décret n° 2019-1271, la France modifie son système de protection du secret de la défense nationale, passant de trois à deux niveaux de classification: Secret et Très Secret.

3 questions à...

Nicolas de Maistre

Directeur de la protection
et de la sécurité de l'État (PSE)

Comment la direction PSE a-t-elle participé à la gestion de la crise sanitaire ?

Le SGDSN, en théorie, n'a pas de rôle dans la conduite de la gestion de crise. En amont, il cherche à anticiper les risques et menaces, conçoit des plans et une organisation, forme les acteurs et organise des exercices. Dans les faits, le SGDSN est forcément un des acteurs de la gestion des crises dans leur dimension interministérielle, mais sans rôle prédéterminé. Son rôle se construit en fonction des besoins et de la nature de la crise.

Avec son expérience en planification et en préparation aux crises, le SGDSN a ainsi appuyé la conduite stratégique de la gestion de la crise sanitaire, participé à la coordination interministérielle dans le champ non sanitaire (mise en œuvre des plans de continuité d'activité notamment), animé et participé à la fonction « anticipation », contribué de façon active à la problématique des masques et renforcé les effectifs là où cela était nécessaire.

L'usage malveillant de petits drones est une préoccupation des autorités françaises. Comment le SGDSN agit-il en la matière ?

Depuis 2014, la question de la lutte anti-drones constitue une priorité pour le SGDSN. Les travaux interministériels qu'il a pilotés ont permis la préparation, en 2015, du rapport du Gouvernement au Parlement qui s'est traduit par le vote de la loi n° 2016-1428 du 24 octobre 2016 relative au renforcement de la sécurité de l'usage des drones civils. Sous l'égide du SGDSN, les textes permettant la mise en œuvre de ces dispositions législatives ont été publiés dont notamment ceux relatifs à l'enregistrement et l'immatriculation des drones, la formation des télépilotes, l'obligation d'équiper les drones de plus de 800 grammes d'un signalement électronique.

La prochaine étape est la publication des arrêtés permettant le déploiement du système d'information étatique (SIE « Infodrone »), chargé de recevoir les signaux électroniques.
Parallèlement, le cabinet du Premier

ministre a chargé le SGDSN de coordonner la gouvernance du dispositif de lutte anti-drones, dans la perspective des échéances à venir : présidence française de l'Union européenne en 2022, coupe du monde de rugby en 2023, Jeux olympiques et paralympiques de 2024. Dans ce cadre, le SGDSN travaille sur la base du triptyque « détection/classification/neutralisation ». Une matrice de gouvernance a été conçue, en lien avec les ministères concernés (ministère de l'intérieur, ministère des armées, ministère de la transition écologique). À ces fins, PSE préside des réunions tous les deux mois afin de suivre l'avancée des sujets d'intérêt. Un point spécifique est également présenté au cabinet du Premier ministre tous les six mois, lors des réunions de la commission interministérielle de la sûreté aérienne (CISA), permettant ainsi d'arbitrer les points faisant débat.

Comment le SGDSN a-t-il préparé l'entrée en vigueur de la nouvelle version de l'IGI 1300 ?

À la suite de la publication de l'arrêté du 13 novembre 2020 portant approbation de l'instruction générale interministérielle (IGI) 1300, la réforme de la protection du secret est entrée en vigueur le 1er juillet 2021.
Pour accompagner pleinement cette réforme et faciliter son adoption et son assimilation, plusieurs supports ont été élaborés et adressés à l'ensemble des hauts fonctionnaires de défense et de sécurité (HFDS) : plaquettes et vidéos institutionnelles de présentation de la réforme, fiches « réflexe » s'adressant aux différents publics cibles, actualisation de la page internet du SGDSN.

Parallèlement, le SGDSN a porté des projets structurants et innovants pour améliorer la protection du secret de la défense nationale : élaboration d'un référentiel commun des enquêtes d'habilitation, structuration de l'offre de formation et dématérialisation des procédures d'habilitation.

À l'international, la réforme des niveaux de classification français (suppression du niveau Confidentiel défense) vise à répondre aux besoins accrus d'échanges avec les partenaires étrangers et à mettre fin aux distorsions préjudiciables constatées entre les mesures de sécurité mises en place par la France et ses partenaires au titre des accords de sécurité en vigueur.

Pour que cet alignement devienne effectif, la direction a engagé la révision d'une quarantaine d'accords intergouvernementaux encadrant l'échange d'informations classifiées entre la France et ses partenaires étrangers. Enfin, la question de la communicabilité des archives de la défense nationale a été traitée, à la demande du Président de la République, par un texte de loi à l'été 2021, suite à une longue concertation des professionnels. L'IGI 1300 a ainsi été modifiée en conséquence.

▶▶▶

Capacités civiles et sécurité nationale

Le SGDSN a clôturé au mois de juillet 2020 le contrat général interministériel (CGI) initié pour 5 ans par le *Livre blanc sur la défense et la sécurité nationale* (LBDSN) de 2013 avec pour objet de « fixer les capacités civiles nécessaires aux missions relatives à la sécurité nationale ». Le CGI 2015-2019 affiche un bilan positif avec 52 % des actions finalisées, 38 % en cours et 10 % restant à engager. L'objectif financier est quant à lui réalisé à 99,6 %, dont près de 20 % de crédits abondés par le SGDSN, soit 12 millions d'euros. Pour pérenniser ces capacités acquises par les ministères, mais aussi pour faire face spécifiquement à des menaces nucléaires, radiologiques, bactériologiques et chimiques (NRBC) en évolution permanente, il était indispensable d'inscrire les efforts dans le temps. C'est l'objet d'un mandat reçu du cabinet du Premier ministre pour prolonger le volet NRBC du CGI en le transformant en un contrat capacitaire interministériel (CCI) de lutte contre le terrorisme NRBC pour la période 2020-2024, couvrant ainsi les Jeux olympiques et paralympiques de 2024. Ce nouveau contrat acte ainsi la poursuite des efforts engagés depuis 20 ans dans le domaine de la lutte NRBC.

Appuyer la gestion de la crise sanitaire

La direction de la protection et de la sécurité de l'État (PSE) a orienté son travail autour de deux axes principaux : la planification interministérielle et la coordination des administrations. S'agissant de la planification interministérielle, le code de la défense dispose que le SGDSN « élabore la planification interministérielle de défense et de sécurité nationale, veille à son application et conduit des exercices interministériels la mettant en œuvre ». C'est à ce titre que les six versions du plan pandémie grippale ont été élaborées sous l'égide du SGDSN depuis 2003, date à laquelle est apparu le virus H5N1 en Asie, responsable de la grippe aviaire. Durant la crise du Covid-19, le SGDSN a notamment contribué à l'élaboration d'une planification « à chaud » à travers le guide d'aide à la décision stratégique (28 février 2020), du plan de déconfinement (5 mai 2020) et de la stratégie de réponse ciblée et graduée à une reprise épidémique (19 juin 2020).

Concernant la coordination interministérielle dans la crise, des actions spécifiques d'adaptation aux évolutions d'une pandémie inédite dans sa nature et dans son ampleur ont été conduites. Dans ce cadre, le SGDSN a :

- animé le réseau des hauts fonctionnaires de défense et de sécurité (HFDS), interlocuteurs permanents et privilégiés du SGDSN au sein de chaque ministère pour la recension de leurs besoins et le suivi de leur plan de continuité d'activité ;
- contribué à la montée en puissance du dispositif interministériel de gestion de crise d'une part en participant directement aux fonctions « décision » et « anticipation » des différentes structures et, d'autre part, en mettant des experts de haut niveau, civils et militaires, à la disposition du ministère des solidarités et de la santé.

Sur le sujet plus particulier des masques de protection, le rôle du SGDSN a principalement porté sur :

- la mobilisation de la production nationale de masques ;
- le lancement des travaux liés au développement de masques destinés au grand public en créant un groupe de travail « innovation », en lien avec la filière textile ;
- la centralisation de l'expression de besoin des ministères ;
- l'élaboration des propositions de recommandations de la répartition des masques au sein des ministères. ◀

Chiffres clés 2019-2020

4
postures semestrielles *VIGIPIRATE*
ainsi que 2 postures en réaction (en janvier 2020 à la suite d'une faille informatique importante ; le 29 octobre 2020 passage au niveau « urgence attentat » après l'attentat de Nice) élaborées et diffusées.

Depuis mars 2019, plus de
300
agents de l'ensemble des ministères formés à armer la CIC et les centres opérationnels des ministères dans le cadre du programme de **professionnalisation des acteurs de la gestion de crise (PAGC).**

2 500
demandes d'habilitation
autorisant l'accès aux informations classifiées au niveau Très Secret faisant l'objet d'une classification spéciale traitées en 2020.

43
accords généraux de sécurité (AGS) à renégocier dans le cadre de la nouvelle IGI 1300.

652
notes d'analyses et fiches techniques rédigées par le Bureau Veille et Alerte (BVA).

120
solutions technologiques
de sécurisation des grands événements labellisées par le comité stratégique de filière (CSF) pour les industries de sécurité.

6
projets sélectionnés
dans le cadre de l'appel à projets de l'agence nationale de la recherche (ANR) et du SGDSN pour les Jeux olympiques et paralympiques de 2024, pour un montant d'aide publique de 2,8 M€.

Disposer des ressources et des moyens de notre performance

Le bureau infrastructure et maintenance du SAG a mené sur 2020 d'importants travaux, notamment sur le site de l'Hôtel national des Invalides.

Le service de l'administration générale (SAG)

Service à vocation transversale du secrétariat général de la défense et de la sécurité nationale (SGDSN), le SAG anime et coordonne l'ensemble des activités administratives et financières des différentes directions et services et leur apporte un soutien dans les domaines logistique et d'infrastructure, ainsi qu'en termes de sécurité.

Pour assurer ses missions, le SAG s'appuie sur une centaine de personnels de statuts divers (fonctionnaires, militaires, contractuels) répartis au sein de trois structures :

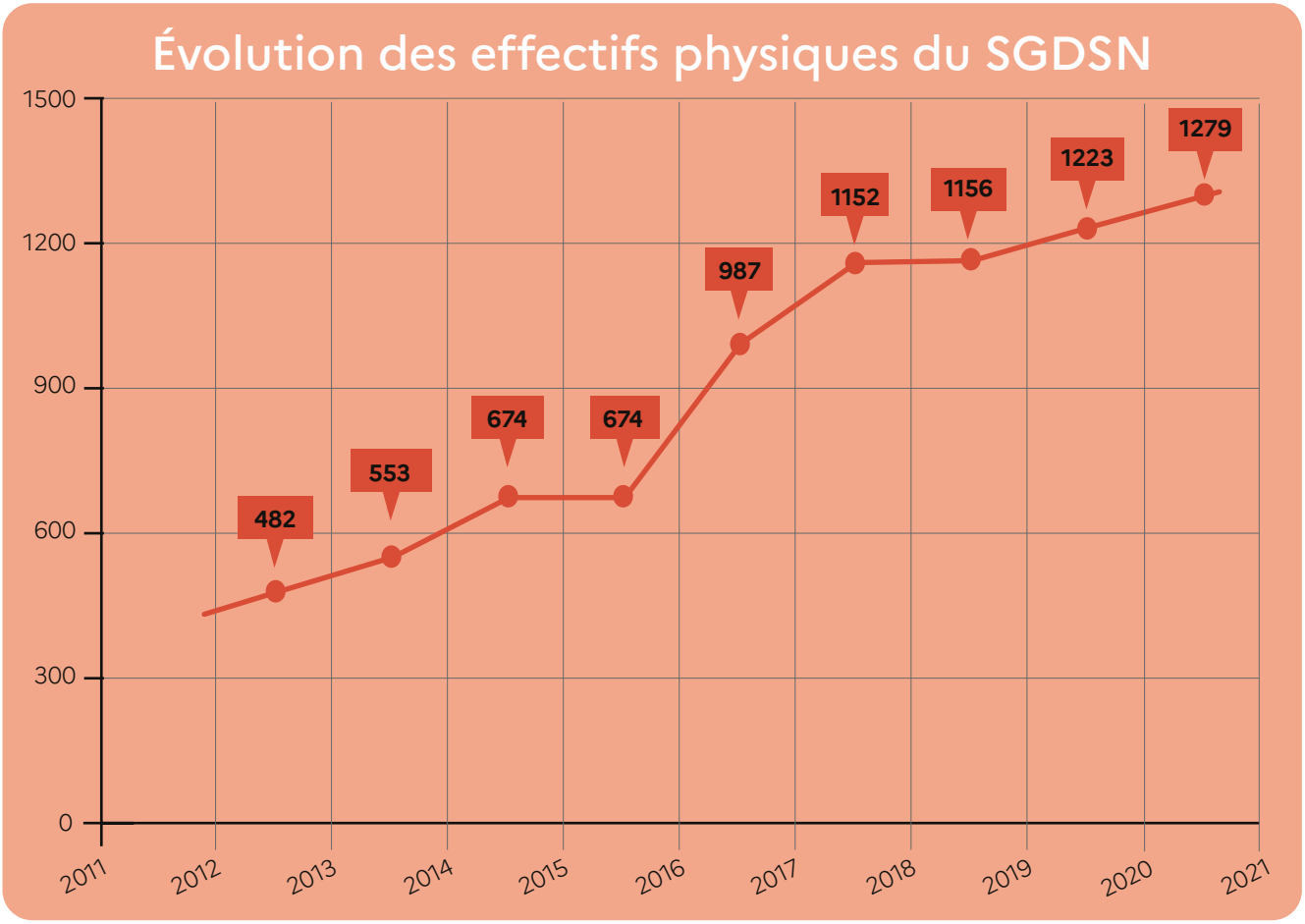
- une sous-direction des affaires financières ;
- une sous-direction de l'administration générale et des ressources humaines, organisée en deux divisions (ressources humaines ; moyens généraux) ;
- un détachement de sécurité.

Cette organisation a été modifiée en 2021.

Finances

Les budgets 2019 *(310 M€ en AE et 293 M€ en CP)* et 2020 *(309 M€ en AE et 276 M€ en CP)* confortent le SGDSN dans ses missions. La période 2019-2020 a été marquée par plusieurs évènements :

- les travaux préparatoires puis la création de l'opérateur des systèmes d'information interministériels classifiés (OSIIC), par décret du 1er juillet 2020. Cette création a eu des incidences significatives sur le plan financier (segmentation des budgets ouverts en loi de finances initiales pour 2020) et des ressources humaines (notamment, le partage du schéma d'emploi de l'ANSSI et la réaffectation des agents civils et militaires dans la nouvelle entité) ;
- la fermeture, le 31 décembre 2020, de l'Institut national des hautes études de sécurité et de justice (INHESJ), établissement public administratif placé sous la tutelle du SGDSN (dotation de 6,1 M€ en 2020), dont l'ensemble des missions sont désormais reprises par le nouvel Institut des hautes études du ministère de l'intérieur (IHEMI). 1 M€ est transféré de façon pérenne au ministère de l'intérieur afin d'assurer le financement pour l'avenir de l'enquête *Cadre de vie et sécurité*, dont l'exploitation sera désormais largement assurée par le service statistique de ce ministère, sous le contrôle méthodologique de l'Autorité de la statistique publique ;
- la réalisation d'un important travail de rénovation de la nomenclature de comptabilité budgétaire du SGDSN, permettant de réduire le nombre de lignes de gestion et de suivi budgétaire et d'apporter par la suite un surcroit de lisibilité de l'activité de la structure et de ses composantes.



Ressources humaines

Le SGDSN se caractérise par la richesse de ses talents, qui repose notamment sur la très grande diversité de ses agents, témoignant du caractère atypique de cette institution, à la fois administration de « missions » et opérateur de l'État.

L'essentiel de la politique des ressources humaines est structuré par cette caractéristique qui implique un taux de renouvellement annuel des effectifs important, un pourcentage élevé d'agents de catégorie A et une grande variété de statuts.

La garantie du maintien d'un flux de personnels suffisant, la prise en compte des carrières des fonctionnaires issus de divers ministères et la gestion des contrats de personnels non titulaires constituent les principaux impératifs de la politique des ressources humaines.

Pour accompagner la réalisation de ses missions, les effectifs du SGDSN ont augmenté (+ 52 ETP en 2019 et + 55 ETP en 2020) et le plan de transformation des ressources humaines issu du plan stratégique 2019-2022 du secrétariat général de la défense et de la sécurité nationale, lancé en 2019, a servi de levier, permettant de développer une stratégie des ressources humaines adaptée aux ambitions du SGDSN.

Les enjeux à venir pour le SGDSN sont le défi du recrutement, dans un contexte fortement concurrentiel s'agissant en particulier des métiers du numérique, et l'accompagnement des parcours professionnels, avec des moyens ambitieux alloués à la formation, notamment.

L'amélioration des pratiques du SGDSN en matière de fidélisation des agents et la communication sur les dispositifs d'aide à la reconversion constituent des axes de progrès.

Enfin, le secrétariat général de la défense et de la sécurité nationale s'engage résolument en faveur de la diversité et de l'égalité professionnelle femmes - hommes (voir le chapitre consacré au projet de transformation RH du SGDSN). ▶▶▶

3 questions à...

Philippe Decouais

Chef du service d'administration générale (SAG)

Alors que les missions du SGDSN évoluent et que son organisation se transforme, quels sont les types de profils recherchés ?

Ces dernières années, plusieurs transformations majeures ont marqué le SGDSN. Je pense notamment à la création de l'ANSSI (2009), l'adossement du CTG (2014) puis du GIC (2016) et à la création de l'OSIIC (2020), occasionnant une extension des missions et une croissance soutenue des effectifs. Une grande diversité de postes est à pourvoir chaque année au regard de l'éventail des missions confiées au SGDSN. Pour l'année 2020, 273 personnes ont été recrutées.

Compte tenu de l'évolution de la menace et des enjeux, l'ANSSI recrute dans des domaines très variés allant de la cryptographie à la détection d'intrusions, en passant par l'accompagnement juridique, le pilotage de projets informatiques ou encore la coordination internationale.

À l'OSIIC, différents profils sont recherchés dans les domaines informatiques : architecte réseaux et télécoms ; expert réseaux : ingénieur réseaux et télécoms ; intégrateur d'application logiciel ; administrateur systèmes et réseaux...

Pour sa part, le GIC a d'importants besoins dans le domaine de la conduite de projets informatiques.

Face à l'ampleur et à la diversité de ses besoins, notamment dans des métiers en tension, le SGDSN a entamé dès 2019 une démarche de « transformation RH » destinée à optimiser les processus de recrutement et de formation et à mettre en place une gestion prévisionnelle des emplois et des compétences (GPEC).

Le SAG s'articule autour de plusieurs bureaux. Comment appuient-ils les agents du SGDSN ?

Les personnels du SAG soutiennent l'ensemble des agents des directions et entités. Une profonde volonté de servir anime chacune des équipes composant ces bureaux. Cette fonction « soutien » se doit d'être réactive et performante quels que soient les sujets traités (RH, logistique, finances,…), tout en démontrant une capacité d'adaptation et d'innovation. Les projets de transformation RH et de transformation numérique sont autant de leviers qui visent à rendre le pilotage du soutien plus efficace et à accroître la flexibilité des modes de fonctionnement.

En matière de formation, le SAG assure la centralisation des expressions de besoins et met en œuvre tous les dispositifs à sa disposition afin de répondre aux attentes des directions et des agents (conventions avec l'IGPDE, commande auprès de prestataires divers, ...). Le SAG dispose d'une conseillère en évolution professionnelle dont les différents dispositifs d'accompagnement sont reconnus (PASS, point de carrière, *coaching*…) et permettent à l'agent de se projeter dans sa carrière.

L'environnement de travail des agents fait l'objet d'une attention particulière. Des budgets importants ont été consacrés à l'aménagement des bureaux et des espaces communs. Le SAG accompagne également financièrement les évènements de cohésion. Outre cet aspect, il met tout en œuvre pour garantir les conditions d'hygiène et de sécurité des locaux et des personnels.

Enfin, la forte croissance des effectifs s'accompagne d'une action sociale résolue ; le SAG multiplie les initiatives en ce sens depuis plusieurs années.

Comment la gestion RH du SGDSN s'inscrit-elle dans la feuille de route SIRH 2022 de la fonction publique ?

La feuille de route SIRH de la fonction publique vise notamment à consolider les systèmes d'information RH, à dématérialiser et fluidifier les processus, à rendre les agents acteurs de leur propre gestion et à disposer d'outils performants et partagés de pilotage de la fonction RH.

Le SGDSN s'inscrit pleinement dans ces objectifs, déclinés dans son plan stratégique 2019-2022 qui prévoit :

- le portage du logiciel de gestion des congés dans l'environnement Extranet du SGDSN, permettant désormais un accès nomade à l'ensemble des agents, notamment ceux en télétravail ;
- la gestion de la paie dans l'environnement Extranet, ce qui ouvrira des possibilités de télétravail aux agents gestionnaires ;
- la dématérialisation du processus de recrutement, inaugurée par l'ANSSI, qui sera prochainement étendue à l'ensemble des directions et services du SGDSN ;
- l'implantation d'un SIRH à partir de 2022.

Le bureau logistique a réalisé 25 mises en configuration de salles de réunion en 2020.

Soutien

La sous-direction « administration générale et ressources humaines » assure les missions techniques et logistiques dans les domaines suivants :

- conduite des travaux d'infrastructure ;
- maintenance des installations techniques ;
- mise en œuvre et maintenance des moyens d'impression et reprographie ;
- gestion d'un centre de documentation ;
- gestion de la « fonction transport » ;
- traitement du courrier pour l'ensemble du SGDSN ;
- gestion des archives ;
- logistique des matériels communs.

Les années 2019 et 2020 sont principalement marquées :

- par la réalisation du schéma directeur immobilier qui a permis la concrétisation d'importantes opérations d'infrastructure tant au sein de l'Hôtel national des Invalides, pour accompagner la création de l'OSIIC, que sur le site d'entreposage de Pantin ;
- dans le cadre du plan stratégique SGDSN 2019-2022, par le lancement du projet de transformation numérique qui vise à gagner en simplicité, en réactivité et partage de l'information, projet dans lequel le service de l'administration générale s'investit ;
- par le recrutement d'une chargée de prévention en 2020 qui, au-delà des actions de fond, a mis en œuvre les mesures de protection contre la Covid-19.

Focus Covid-19

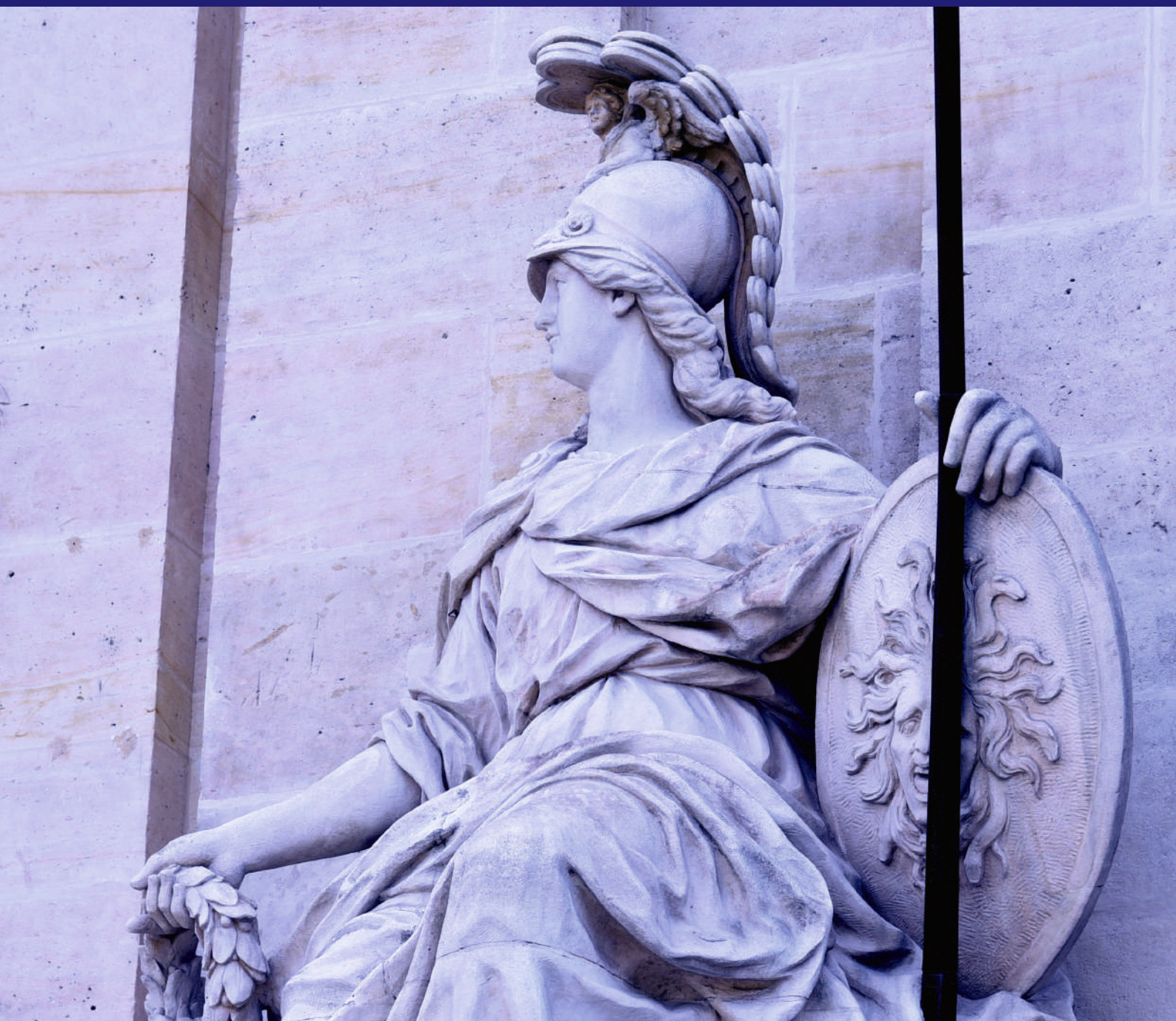
Comme l'ensemble des personnels du SGDSN, le SAG a été particulièrement mobilisé pour assurer la continuité du service tout au long de l'année 2020. Dès le franchissement du stade 2 de l'épidémie de Covid-19 en mars 2020, le SAG a adapté son organisation pour répondre aux attentes des directions et de leurs personnels, notamment dans le domaine logistique.

Sur le plan sanitaire, la chargée de prévention a procédé à différentes actions sur les sites du SGDSN (campagnes d'affichage, mise en place de jauges pour les salles de réunions, suivi des cas individuels, élaboration de procédures avec la médecine de prévention). L'année 2020 a ainsi permis l'émergence d'une véritable fonction « prévention » au sein du SGDSN.

Les bureaux du SAG ont assuré la continuité de la paie des personnels, des achats et des paiements associés, dont ceux en régie, en maintenant une présence significative sur site compte tenu des contraintes de confidentialité nécessitant l'usage de réseaux sécurisés, inaccessibles en mobilité.

Une attention particulière a été également portée au traitement rapide des factures : le délai global de paiement des factures, qui ne doit pas excéder 30 jours, a été en 2020 de 14,6 jours, en amélioration de 8 % par rapport à 2019. De plus, les délais contractuels de réalisation des prestations ont été adaptés, lorsque cela s'est avéré nécessaire. ◀

Sécuriser nos systèmes d'information



Une menace en pleine expansion

Les années 2019 et 2020 ont été marquées par un net accroissement des cyberattaques de tous types : cybermalveillance, espionnage, rançongiciel, sabotage. La transformation numérique, source de spectaculaires évolutions, génère donc aussi de nouveaux risques dont rien ne permet de prévoir l'amoindrissement à court terme.

En 2020, la cybermalveillance est par ailleurs apparue comme étant la première menace à laquelle entreprises et collectivités ont eu à faire face.

Pour sa part, l'ANSSI a traité quatre fois plus d'attaques par rançongiciels en 2019 et 2020 que lors des années précédentes. 39 % de ces attaques étaient dirigées contre des établissements ou des professionnels du secteur de la santé. 20 % ont été dirigées contre des collectivités locales ou territoriales.

Plus généralement, l'agence a été saisie de 2 287 signalements d'anomalies, conduisant à l'examen de 759 incidents dont 7 se sont avérés être particulièrement préoccupants. Parallèlement, 20 opérations de cyberdéfense ont été menées.

Face à l'accroissement de la menace, des décisions ont été prises au plus haut niveau de l'État. 1 milliard d'euros seront mobilisés dans la mise en œuvre d'une stratégie nationale de cybersécurité, dont 720 millions d'euros de fonds publics.

Chiffres clés
(au 31/12/2020)

548
agents civils et militaires,

un budget de

21
millions d'euros
(hors masse salariale)

ainsi que le pilotage de

136
millions d'euros
(volet cybersécurité de France Relance)

20
opérations de cyberdéfense en 2020

246
visas de sécurités délivrés.

Extension de l'ANSSI

Au cours de la période 2019-2020, l'ANSSI a préparé son installation sur de nouveaux sites. Le principal sera l'antenne rennaise dans laquelle l'ANSSI s'implantera progressivement à partir du mois de septembre 2021. Accueillant 200 personnes à terme, cette antenne aura pour premier objectif de renforcer les échanges avec les partenaires privilégiés déjà installés à Rennes : ministère des armées, commandement de la cyberdéfense (COMCYBER), direction générale de l'armement (DGA), industriels et *start-up*. Cette implantation permettra également d'absorber la croissance planifiée des effectifs de l'ANSSI au cours des prochaines années, tout en offrant des parcours de carrière variés aux agents.

L'ANSSI a également préparé la création d'un Campus Cyber. Initié par le Président de la République, le Campus Cyber a pour objectif de rassembler et de fédérer acteurs privés, publics et associatifs de l'écosystème de la cybersécurité, au sein d'un lieu unique, afin de développer des coopérations et de promouvoir une « excellence française ». Ce projet a connu des développements importants en 2020 : une centaine d'acteurs, dont l'ANSSI, a rallié le projet et le lieu d'implantation a été choisi. Le Campus s'installera dans la tour Eria, localisée sur le site de Paris La Défense, à Puteaux (92).

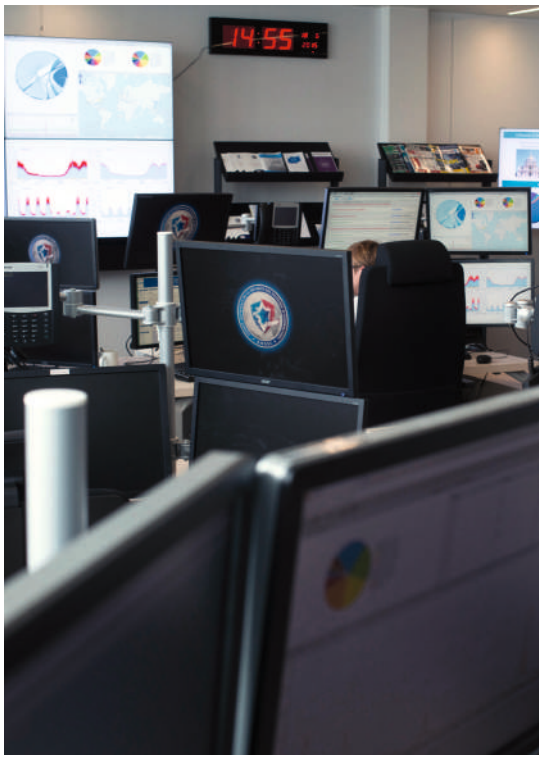
Les équipes de l'ANSSI sont présentes sur le site de l'Hôtel national des Invalides et au sein de la Tour Mercure. Une partie des agents rejoindra également l'antenne de Rennes et le Campus Cyber.

Cybersécurité européenne

L'ANSSI a poursuivi sa mission de conseil et a continué à promouvoir, notamment dans la perspective de la présidence française de l'Union européenne en 2022, la construction d'un espace numérique sécurisé et de confiance à l'échelle européenne. Les 2 et 3 juin 2019, la France a accueilli la première édition de l'exercice de haut niveau *Blue OLEx*. Soutenus par l'Agence européenne de cybersécurité (ENISA) et la Commission européenne, les chefs des autorités nationales de cybersécurité de 23 États membres de l'UE se sont réunis à Paris pour un exercice commun. L'édition 2020 a été marquée par la création de CyCLONe (*Cyber Crisis Liaison Organisation Network*). Maillon stratégique du dispositif, ce réseau de coordination créé à l'initiative de la France et de l'Italie rassemble les responsables des autorités nationales de cybersécurité de l'Union européenne.

Le 7 juin 2019, le Conseil de l'Union européenne a adopté le règlement (UE) 2019/881 sur la cybersécurité. Véritable avancée pour l'autonomie stratégique européenne, ce règlement a deux objectifs principaux. D'une part, il accorde un mandat permanent à l'ENISA, avec davantage de ressources et de nouvelles prérogatives. D'autre part, il crée un cadre européen de certification en matière de cybersécurité, élément essentiel pour le renforcement de la sécurité du marché unique numérique européen.

Dans la lignée de l'adoption par le Conseil de l'Union européenne de la loi sur la cybersécurité en juin 2019, la Commission européenne a publié le 16 décembre 2020 la nouvelle stratégie de cybersécurité de l'Union européenne. Celle-ci, qui contribuera au renforcement de la souveraineté européenne, contient notamment un « paquet cyber ». Ce « paquet » comporte une proposition de révision de la directive *Network and Information Security* ainsi qu'un rapport sur la mise en place des recommandations de la boîte à outils 5G. De plus, face à l'accroissement de la cybermenace et pour affirmer la souveraineté européenne en matière de numérique, la Commission européenne a proposé un règlement visant à renforcer la cybersécurité des institutions européennes.



France Relance

Le 3 septembre 2020, l'ANSSI s'est vue confier le pilotage du « volet cybersécurité » du plan France Relance. Au niveau territorial, ce plan doit permettre d'accélérer le développement des équipes informatiques de proximité (CSIRT) destinées à assister le tissu économique et social local. Ce plan doit également placer les équipes régionales de réaction aux incidents informatiques (CERT) au cœur des dynamiques locales. Les CERT régionaux seront donc les interlocuteurs des acteurs locaux désireux d'élever leur niveau de cyberdéfense dans le cadre du plan de relance : PME, ETI, communes de plus de 5 000 habitants et intercommunalités. ◄

Cyber Festival : les 10 ans de l'ANSSI

Le 4 juin 2019, le Cyber Festival organisé par l'ANSSI à l'occasion de ses 10 ans a permis d'annoncer trois pistes stratégiques, pour l'agence comme pour l'écosystème national de la cybersécurité : la formation, qui doit permettre de contribuer à alimenter cette filière d'avenir ; la donnée, ensuite, dont l'exploitation doit nous permettre d'inventer la cybersécurité de demain ; la co-construction, enfin, dont l'efficacité a déjà fait ses preuves et qui doit devenir la norme. ◄

3 questions à...

Guillaume Poupard

Directeur général de l'agence nationale de la sécurité des systèmes d'information (ANSSI)

La cybermenace a-t-elle été affectée par la crise sanitaire ?

Affectée... oui, mais pas au sens où nous l'aurions souhaité ! Comme il en va de tout événement exceptionnel, la petite cybercriminalité exploite la crise sanitaire et le besoin d'information sur la pandémie et utilise des techniques habituelles d'usurpation de qualité pour dérober des données personnelles ou de connexion. Le nombre de courriels malveillants et d'escroqueries sur le thème de la Covid-19 a donc fortement augmenté. L'ANSSI fait le constat d'un accroissement très rapide du niveau de la cybermenace en France. Dans la continuité d'une trajectoire initiée en 2019, le nombre de cyberattaques a explosé : le nombre de victimes a ainsi été multiplié par 4 en un an. C'est très préoccupant.

Des structures hospitalières ont été victimes de cyberattaques. Comment l'ANSSI s'est-elle positionnée pour les aider à y faire face ?

Effectivement, plusieurs établissements ont été ciblés par des groupes d'attaquants en 2020. Les conséquences de ces cyberattaques sur les capacités opérationnelles des hôpitaux ont parfois été très importantes et les ont obligés à fonctionner en mode dégradé, avec un retour aux « papiers et crayons ».

Pour tirer les conséquences de ces attaques – on mesure bien les risques induits par une paralysie des hôpitaux – le volet cybersécurité du plan France Relance consacre 25 millions d'euros au secteur de la santé. Dans ce cadre, l'ANSSI propose aux établissements de santé des « Parcours de cybersécurité ». Elle pose un diagnostic de cybersécurité, puis elle les aide à atteindre le niveau de sécurité adéquat, notamment au travers d'actions de sensibilisation et de formation. Elle leur propose aussi un ensemble de mesures organisationnelles et techniques de cybersécurité. Quatre niveaux de parcours sont proposés, afin de faire face à toutes les situations de départ.

La création d'un centre d'information spécifique, le CERT-Santé, constitué à partir de la cellule d'accompagnement cybersécurité des structures de santé (ACSS) de l'Agence du numérique en santé, permettra de coordonner les différentes parties prenantes, de surveiller l'exposition des établissements de santé aux vulnérabilités identifiées et de mutualiser les expériences.

Mais pour faire fonctionner convenablement ce qui est en cours de structuration, il faut avant tout mener un travail de sensibilisation de tous les acteurs de la santé. Cette sensibilisation se fera *via* des campagnes, mais aussi en intégrant la cybersécurité dans les cursus de formation des personnels de santé.

Quelles sont les bonnes pratiques prônées par l'ANSSI pour limiter les risques ?

Avant toute chose, il faut consulter les guides de l'ANSSI disponibles sur ssi.gouv.fr : *guide des bonnes pratiques de l'informatique*, *guide d'hygiène informatique*, *guide pour les dirigeants*, *guide cartographie*... Ensuite, en étant bien accompagné, on peut :

- faire un état des lieux réguliers de ses systèmes pour mettre en œuvre des actions concrètes ;
- former et sensibiliser ses collaborateurs, notamment avec le cours en ligne SecNumAcadémie de l'ANSSI ;
- faire appel à des prestataires et utiliser des produits de sécurité labellisés « de confiance », grâce au visa de sécurité ANSSI ;
- s'entraîner à la gestion de crises cybernétiques.

Enfin, les dirigeants doivent prendre conscience de l'importance de la cybersécurité, en intégrant le risque cybernétique dans leur planification de sécurité, au même titre que d'autres risques. La croissance de la menace, la vulnérabilité de nombre d'infrastructures informatiques et le coût financier pour la victime d'une attaque menée à bien font de ce risque une menace de niveau stratégique.

Concevoir des outils numériques au service de l'interministériel

3 questions à...

Vincent Strubel

Directeur de l'opérateur
des systèmes d'information
interministériels classifiés
(OSIIC)

À quels objectifs répond la création de l'OSIIC ?

La création de l'OSIIC, issue des réflexions conduites par le SGDSN – au titre de son plan stratégique – a été constituée par le rassemblement du centre de transmissions gouvernemental (CTG) et de la sous-direction numérique (SDN) de l'ANSSI. Cette fusion vise à offrir un gain de lisibilité et d'efficacité, et à permettre la mise en œuvre de synergies utiles, dans chacune des trois missions principales que se partageaient ces deux structures antérieures et qui sont désormais reprises par l'OSIIC :

- la conception et la mise en œuvre, en tout temps et en tout lieu, de moyens de communication classifiés spécifiques au profit du Président de la République et des très hautes autorités gouvernementales ;
- la conception, le déploiement et l'exploitation de systèmes d'information classifiés interministériels, au profit de l'ensemble des ministères et de certains opérateurs d'importance vitale ;
- la fourniture d'une offre de services numériques communs à l'ensemble du SGDSN, dans un rôle de direction numérique de ce dernier.

En charge des systèmes d'information interministériels classifiés, comment l'OSIIC a-t-il été impacté par la crise sanitaire dans la conduite de son activité ?

La crise sanitaire a brutalement accru les besoins en systèmes d'information et de communications interministériels classifiés. Ces besoins nouveaux se sont traduits à la fois par une multiplication des demandes de déploiement, et par des cas d'usages nouveaux, dont le plus emblématique est le recours aux moyens de visioconférence OSIRIS/HORUS pour la tenue en « distanciel » des conseils de défense et de sécurité nationale et des conseils des ministres[1]. Par ailleurs, la densification du réseau OSIRIS, notamment hors de la région parisienne, a permis la tenue d'un nombre croissant de réunions en distance, par des moyens hautement sécurisés.

L'OSIIC a naturellement accompagné ces évolutions, non seulement par l'adaptation des solutions techniques qu'il fournit aux ministères et aux très hautes autorités de l'État, mais aussi par son soutien aux utilisateurs dans la mise en œuvre de telles solutions.

En tant que DSI, comment l'OSIIC accompagne-t-il le SGDSN ?

En tant que DSI, l'action de l'OSIIC a forcément été guidée par les contraintes induites par la crise sanitaire. Au-delà de la nécessaire transformation numérique du SGDSN, le contexte sanitaire a imposé un recours très fortement accru au télétravail. Cette adaptation a été tout particulièrement délicate à mener pour un organisme comme le SGDSN, dont les principaux outils de travail reposaient sur des systèmes d'information classifiés, par construction non accessible à distance.

Par ailleurs, l'OSIIC ambitionne de consolider, rationaliser et fiabiliser un système d'information en large expansion, afin d'en assurer la maintenabilité dans la durée. L'extension très rapide, à la faveur de la crise sanitaire, du périmètre du système d'information du SGDSN, a exacerbé des fragilités préexistantes de celui-ci. L'OSIIC a par conséquent mené les travaux de cadrage préliminaires pour une refonte en profondeur de ces infrastructures.

1. Ces derniers, s'ils ne sont pas classifiés, revêtent néanmoins une sensibilité particulière, liée au secret des délibérations du gouvernement, qui justifie le recours à des moyens classifiés.

Création de l'OSIIC

Créé le 1er juillet 2020, suite à un travail de concertation interne engagé dans le cadre du plan stratégique 2019-2022, l'opérateur des systèmes d'information interministériels classifiés (OSIIC) est doté initialement de 100 emplois civils et 187 emplois militaires, par regroupement des effectifs du CTG et de la SDN. L'OSIIC doit connaître un renforcement de ses effectifs à hauteur de 10 équivalents temps plein annuels, pour l'amener à un effectif théorique de 317 emplois fin 2023. Cet effectif cible, établi lors de la préfiguration de l'OSIIC, doit lui permettre de répondre à une extension de ses missions, tant dans le domaine interministériel (avec notamment l'élargissement du périmètre de déploiement OSIRIS) que dans son rôle de soutien au profit du SGDSN, pour répondre notamment à l'accroissement des effectifs de ce dernier et à l'extension de l'ANSSI sur de nouveaux sites. Il est par ailleurs doté d'un budget initial de 22 M€ en autorisations d'engagement et 23 M€ en crédits de paiement.

Septembre 2020, cérémonie de lancement de l'OSIIC.

Consolidation des capacités

La création de l'OSIIC et la phase de préfiguration qui l'a précédée se sont déroulées dans le contexte de la crise sanitaire, source à la fois d'une charge fortement accrue pour ses équipes et de contraintes dans la conduite du changement.

Cette consolidation a reposé en premier lieu sur le regroupement des équipes sur un site unique et sur un important effort de recrutement. Ces recrutements ont servi à compenser certains départs liés à la fusion des deux structures et surtout à doter l'OSIIC des fonctions de soutien (ressources humaines de proximité, communication interne, suivi budgétaire) qui lui manquaient initialement. En l'absence de forums de recrutement en présentiel, cet effort a principalement reposé sur une communication active sur les réseaux sociaux, couronnée de succès puisqu'elle a permis à l'OSIIC de réaliser son schéma d'emploi et de se doter des fonctions nécessaires. Un plan de formation ambitieux a également été élaboré, afin d'uniformiser les compétences des équipes et de favoriser les transferts d'activité indispensables à l'optimisation des capacités de l'OSIIC. Celui-ci prévoit la réalisation d'environ 240 formations individuelles en 2021. Une réflexion stratégique a par ailleurs été menée afin de définir les orientations de l'OSIIC et les enjeux qu'il doit relever. Celle-ci a permis l'élaboration d'un schéma directeur, finalisé en janvier 2021, qui fixe les ambitions de l'OSIIC à trois ans, et une trajectoire de référence adossée à des objectifs trimestriels.

Un travail de consolidation des capacités logistiques de l'OSIIC a également été mené de manière prioritaire, avec la mise en service en octobre 2020 d'une nouvelle plateforme logistique à Pantin, puis la reprise dans un inventaire unifié et le transfert de l'ensemble des stocks (matériels informatiques et réseaux) de l'OSIIC sur ce site, qui devrait permettre des gains d'efficacité significatifs dans le déploiement des systèmes tant interministériels que propres au SGDSN. ▶▶▶

▶▶▶

Décembre 2020, le Président de la République en visioconférence, grâce aux outils mis au point par les équipes de l'OSIIC.

Schéma directeur

Devenu le principal instrument de pilotage des actions à long terme de l'OSIIC, le schéma directeur fixe les ambitions à trois ans et une trajectoire de référence adossée à des objectifs trimestriels. Ces ambitions portent notamment sur :

- le déploiement d'infrastructures simplifiées et rationalisées, plus fiables et évolutives, pour l'ensemble des services opérés par l'OSIIC, en mutualisant autant que possible les services issus de la SDN et du CTG ;
- la mise en place d'une offre de service rénovée au profit de l'ensemble des bénéficiaires, tirant les leçons de la crise sanitaire ;
- une optimisation du fonctionnement interne ;
- une relation réinventée avec les bénéficiaires des services de l'OSIIC, autant qu'avec ses partenaires dans l'écosystème numérique de l'État (ANSSI, DINUM (direction interministérielle du numérique), directions numériques ministérielles) afin de favoriser une meilleure prise en compte des besoins, une meilleure compréhension des capacités offertes par les solutions de l'OSIIC et les mutualisations utiles avec d'autres infrastructures numériques.

Ce schéma directeur est devenu le principal instrument de pilotage des actions à long terme de l'OSIIC. Un travail méthodologique a été planifié en 2021 afin d'appuyer ces ambitions, avec notamment la mise en œuvre d'une démarche de pilotage produit sur les principaux services fournis par l'OSIIC et une montée en compétence sur les méthodes Agile et les approches « DevOps » à travers des séminaires internes et un accompagnement ciblé sur certains projets.

Gagner en efficacité : une gouvernance unifiée pour optimiser le déploiement

Afin de gagner en efficacité, l'OSIIC a conduit une refonte de la gouvernance et du pilotage des déploiements de moyens interministériels. Cette gouvernance a été mise en place dès septembre 2020, adossée à un réseau de référents ministériels, garants de la cohérence des besoins de leur ministère, ainsi qu'à des règles de priorisation communes et à un comité stratégique annuel. Elle se traduit par l'élaboration et le suivi d'un « macro-planning » partagé, fournissant à l'OSIIC et aux ministères une visibilité sur les déploiements prévus dans les dix-huit prochains mois.

Combinée à une fluidification des procédures au sein de l'OSIIC, cette nouvelle gouvernance a permis une accélération significative du déploiement de la solution de visioconférence et de téléphonie classifiée OSIRIS, qui a abouti à un quasi-doublement du parc déployé au cours de la première année d'existence de l'OSIIC.

Par ailleurs, la mobilisation croissante des chaînes logistiques ministérielles, et une répartition efficace des tâches entre ces dernières et l'OSIIC ont permis des progrès importants dans la diffusion d'OSIRIS hors de la région parisienne, avec le déploiement de la solution dans les préfectures, gendarmeries et ambassades. Un effort de priorisation particulier a été réalisé pour doter les départements et collectivités d'outre-mer, qui devraient globalement disposer de ces moyens mi-2021. ▶▶▶

Mars 2020, visioconférence du Président de la République avec les 27 Etats-membres de l'Union Européenne.

Développement de la solution Secdroid

Initialement conçue par l'ANSSI, la solution Secdroid, dérivé sécurisé d'Android permettant le déploiement de terminaux smartphones aptes à traiter des informations *Diffusion Restreinte*, a vu son développement transféré à l'OSIIC. Composante essentielle des moyens de mobilité fournis aux agents du SGDSN, elle a joué un rôle primordial dans son adaptation aux nouvelles contraintes sanitaires. Cette solution est également partagée avec le ministère de l'intérieur, qui l'intègre dans sa solution de mobilité Néo, déployée à hauteur de 90 000 terminaux environ au profit des forces de sécurité intérieure.

Cette coopération entre l'OSIIC et le ministère de l'intérieur s'est intensifiée au second semestre 2020, avec la préparation puis la notification du marché « Néo 2 », visant à renouveler le parc de terminaux Néo, et à étendre ce dernier à environ 200 000 terminaux. Outre son implication en 2020 dans l'établissement du cahier des charges et dans l'analyse des offres, l'OSIIC est fortement mobilisé en 2021 afin d'assurer les évolutions nécessaires dans ce cadre de la solution Secdroid, évolutions dont bénéficieront également les utilisateurs du SGDSN à compter de 2022. ◄

Fiabilisation des infrastructures

Comme dans nombre d'autres entités, l'extension très rapide, à la faveur de la crise sanitaire, du périmètre du système d'information du SGDSN, a exacerbé des fragilités préexistantes, qu'il s'agisse d'infrastructures d'hébergement ou d'accès insuffisamment dimensionnés ou redondés, de complexité d'exploitation ou de technologies vieillissantes.

L'OSIIC a par conséquent mené les travaux de cadrage préliminaires pour une refonte en profondeur de ces infrastructures, notamment à travers leur migration depuis des moyens d'hébergement historiques et peu adaptés, vers un *datacenter* conforme à l'état de l'art mis en place conjointement par le SGDSN et le ministère de l'intérieur au sein du Fort de Rosny. Cette migration, qui débutera en 2021, sera l'occasion d'une refonte complète de l'architecture de certains des systèmes migrés, dans un objectif de rationalisation et de simplification de leur exploitation. ►►►

Chiffres clés

799
visioconférences, dont
388
par moyens classifiés,
ont été organisées au profit des
très hautes autorités en 2020,
contre
121
(47 classifiées)
en 2019.

OSIRIS:
700
terminaux déployés
fin 2020

Décembre 2020, conseil des ministres
en visioconférence.

Projet COM GOUV-NG

L'OSIIC a été fortement mobilisé en 2020, et le restera jusqu'à la fin 2021, par le projet COMGOUV-NG de refonte des moyens de communication de l'avion à usage gouvernemental long-courrier (AUG-LC). Ce projet, fortement contraint par le calendrier d'immobilisation de l'appareil, a également subi les conséquences de la crise sanitaire, entraînant de nombreux retards parmi les fournisseurs industriels impliqués. Une mobilisation accrue des équipes de l'OSIIC et de ses fournisseurs à partir du second semestre 2020 devrait cependant permettre le respect des échéances.

À l'issue du projet, l'AUG-LC intégrera un système de communication rénové et offrira une convergence accrue avec les moyens, notamment de visioconférence, fournis par l'OSIIC à l'interministériel, gage tant d'une plus grande facilité d'exploitation que d'une meilleure ergonomie d'utilisation. ◄

Préparation du décommissionnement de RIMBAUD

L'OSIIC assure également le pilotage du réseau RIMBAUD, réseau téléphonique administré par Orange, qui offre un haut niveau de résilience face à différents scénarios de dysfonctionnement ou de saturation. Ce réseau permet actuellement de fournir, aux différentes entités impliquées dans la gestion gouvernementale des crises majeures, des moyens de communication résilients, tant classifiés (terminaux TEOREM) que non classifiés.

Reposant sur des technologies frappées d'obsolescence, le réseau RIMBAUD sera arrêté puis démantelé au plus tard fin 2022. L'OSIIC a par conséquent entamé dès juillet 2020 les études nécessaires au décommissionnement de ce réseau, ainsi qu'une coopération étroite avec la direction interministérielle du numérique (DINUM) et la direction du programme «Réseau radio du futur», en vue d'offrir un niveau de résilience équivalent par le déploiement de moyens classifiés plus modernes (OSIRIS) sur les réseaux usuels de travail des agents publics (Réseau interministériel de l'État, RIE). Cette perspective d'arrêt de RIMBAUD devrait prendre une place prépondérante dans la planification des déploiements de moyens classifiés dès 2021. ◄

Soutenir le groupement interministériel de contrôle

Des responsabilités étendues

Depuis 2016, le groupement interministériel de contrôle (GIC) s'est transformé afin de répondre à l'extension de ses missions et à l'augmentation du nombre de demandes de techniques de renseignement. Le GIC centralise les demandes, suit leur instruction et l'exécution des autorisations délivrées. Il met en œuvre les surveillances numériques en s'interposant entre les opérateurs et les services de renseignement. Les communications électroniques recueillies sont exploitées par les services au sein du GIC, dans ses centres métropolitains et outre-mer. Il en contrôle l'exploitation, détruit les données au terme du délai légal et interrompt les surveillances qui s'écarteraient de l'autorisation accordée. Il exécute les traitements automatisés autorisés visant à détecter des comportements numériques traduisant une menace terroriste. Il installe et administre en outre des systèmes informatiques sécurisés permettant l'exploitation centralisée des données recueillies par les services de renseignement (balises, sonorisations, etc.). Le GIC assure enfin la défense du Premier ministre devant la formation spécialisée du Conseil d'État à laquelle tout particulier s'estimant illégalement surveillé peut adresser un recours.

Assurer la permanence des missions

Pour le GIC, l'année 2019 peut être qualifiée d'année charnière entre une période d'augmentation extrêmement forte de l'activité et une deuxième phase de croissance toujours soutenue, mais plus mesurée. Elle a été, pour la première fois depuis quatre années, l'occasion d'envisager une consolidation des acquis.

La pandémie a eu pour conséquence tragique la perte de l'un des sous-officiers de gendarmerie appartenant au peloton de sécurité du groupement, décédé de la Covid-19. Dans un contexte de sur-occupation de ses locaux et alors que l'essentiel de ses activités est protégé par le secret de la défense nationale, le GIC a su respecter les jauges sanitaires en mettant en place de nouvelles modalités de travail. Grâce à la réactivité que lui confère sa capacité de développement informatique interne, le GIC a déployé dès les premiers jours de la crise des moyens de travail à distance qui, associés à une revue générale des projets, ont permis de déplacer une part importante de l'activité hors des réseaux classifiés internes. En parallèle, le GIC mobilisait toutes les surfaces disponibles pour permettre aux agents des services de poursuivre leur activité d'exploitation du renseignement dans ses locaux protégés. Ainsi, malgré un contexte particulièrement éprouvant, le GIC a assuré la permanence de ses missions et a connu en 2020 un nouveau surcroît d'activité.

Chiffres GIC

235
personnes au 31/12/2020

29,1 M€
CP 2020
consommés, hors fonds spéciaux

Une
Quarantaine
d'emprises, à Paris, en métropole et outre-mer

4000
utilisateurs accèdent aux systèmes d'information protégés du GIC

Près de
350
autorisations par jour

De 2019 à 2020 :
20%
d'augmentation de l'activité de mise en œuvre par le GIC de techniques de renseignement

La technologie au profit des opérations

En 2019, une priorité absolue a été donnée au programme de sécurisation des systèmes informatiques du GIC. En six mois, l'ensemble des échanges opérationnels entre le GIC et les acteurs du numérique a été renforcé par des moyens techniques et des procédures strictes appliquées par tous et supervisées.

En parallèle, une refonte du socle informatique des applications classifiées du GIC a été initiée. Elle a permis de rationaliser des développements déclenchés tous azimuts sous la pression opérationnelle et de les asseoir sur une architecture modulaire afin de faciliter leur maintenance et leurs évolutions. Devenu numérique depuis cinq ans, le GIC s'apprête à devenir *cloud native*.

En 2019, la technique de captation de paroles a été pleinement centralisée, avec des équipements capables également de supporter la centralisation des captations d'images.

Les possibilités introduites par la loi de programmation militaire[1] 2019-2025 ont été concrétisées en 2019, après un travail interministériel visant à tirer toutes les conséquences des nouvelles dispositions. Le GIC s'est mobilisé pour offrir aux services les outils leur permettant de pleinement bénéficier des évolutions du cadre légal.

Année singulière, 2020 n'a aucunement entamé la dynamique du groupement. Si le nombre de techniques de renseignement « au contact » (sonorisations, captations d'images, recueils de données informatiques) a décru, les techniques mises en œuvre par le GIC ont une nouvelle fois connu une forte croissance, de l'ordre de + 20 %. Le GIC a traité 1 739 alertes algorithmiques issues des traitements automatisés, qu'il met en œuvre pour la prévention du terrorisme, et il a noué des contacts opérationnels avec de nombreux nouveaux opérateurs et fournisseurs de services de communications électroniques.

Alors qu'il augmentait la cadence, le GIC a déployé en 2020, au profit des exploitants des services de renseignement, un nouvel outil de valorisation des données de connexion permettant de visualiser les événements de communication sur un fond de carte interactif, de catégoriser les usages numériques des personnes surveillées et de détecter des liens entre affaires.

1. Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

Centralisation dans les serveurs du GIC des données issues des techniques de renseignement

Préparer l'avenir

Avec le commissariat aux communications électroniques de défense, le GIC se prépare à l'avènement des réseaux de communications électroniques de 5e génération. Le passage de la 4G à la 5G se traduit par un changement profond de l'architecture technique chez les opérateurs qui accompagne une révolution des usages, notamment avec la généralisation des objets connectés. Outre le remplacement de tous les équipements techniques chez les opérateurs et au sein du GIC pour maintenir la capacité actuelle d'interception, il conviendra de s'assurer que la loi s'applique à tous les acteurs du numérique.

Pour répondre aux nombreux enjeux technologiques auxquels il fait face, le GIC doit non seulement faire preuve de réactivité opérationnelle mais aussi disposer d'une capacité d'innovation. C'est désormais sur cette dernière qu'il convient de mettre l'accent, afin que le GIC offre aux services de renseignement des outils d'exploitation toujours performants, dans le strict respect du cadre légal. Armé d'une compétence de développement informatique interne, le GIC maîtrise les capacités qu'il déploie, il adapte en continu ses applications à raison de deux mises à jour quotidiennes et consacre une part croissante de ses effectifs à des tâches de conception et d'innovation. Enfin, le GIC se prépare à adopter un fonctionnement nouveau, dans des conditions optimales, lorsqu'une partie de ses agents occupera un nouveau site qui se substituera à la deuxième emprise parisienne du GIC en 2023. Le nouveau bâtiment, actuellement en travaux, hébergera un centre de données supplémentaire.

Le GIC n'a jamais dévié, depuis sa transformation très rapide effectuée en 2016, des missions qui lui avaient été fixées. Il a mis en œuvre chacune des sept évolutions que le cadre légal a connues depuis le socle de 2015 et prépare, dans le respect des principes de ce socle et d'une doctrine qui se consolide, la nouvelle évolution. ◄

Édito par le Général Vincent Cousin

Secrétaire général adjoint de la défense et de la sécurité nationale.

Le SGDSN est une maison centenaire. Sa mission est ancienne, permanente et particulièrement vaste. En effet, le SGDSN est un service du Premier ministre qui travaille en lien étroit avec la Présidence de la République. Il agit en appui de la prise de décision politique, en assistant le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

Son champ d'action est très étendu. Il couvre l'ensemble des questions stratégiques de défense et de sécurité dans les domaines de la programmation militaire ; la dissuasion nucléaire ; la sécurité intérieure concourant à la sécurité nationale ; la sécurité économique et énergétique ; la lutte contre le terrorisme ; la planification des réponses aux crises.

Aujourd'hui, les vieux équilibres géostratégiques auxquels nous nous étions habitués sont sérieusement ébranlés. L'évolution des menaces auxquelles nous faisons face est proportionnelle aux progrès fulgurants de la technologie, en particulier dans le domaine du numérique, et cela a des effets directs sur les stratégies de notre pays. Au sein du SGDSN, il est alors de notre responsabilité, de notre devoir, de nous assurer que notre organisation, notre ressource humaine et nos modes de fonctionnement restent adaptés au rythme opérationnel qui s'impose à nous. Concrètement, il s'agit de s'assurer que notre organisation reste cohérente avec l'évolution de nos missions. Il s'agit aussi d'adapter et d'ajuster le recrutement, la formation et les compétences de tous nos personnels, tout en gardant en tête l'objectif de fidélisation de nos agents. Notre organisation, nous la transformons sans cesse, en l'adaptant aux évolutions de notre environnement. Or cette transformation doit suivre une direction. Cette direction est donnée par le plan stratégique 2019-2022 et s'illustre dans les plans de transformation numérique et de la fonction des ressources humaines, qui produisent leurs premiers effets.

Avec plus de cent ans d'ancienneté, le SGDSN regarde vers l'avenir, pour mieux préparer nos dirigeants, nos concitoyens, notre pays à faire face et répondre aux risques et menaces de nature à remettre en cause de nos intérêts fondamentaux. Avec plus de cent ans d'ancienneté, le SGDSN s'adapte et se transforme, afin d'accompagner ses agents dans la conduite de leurs missions. Faisons nôtres ces mots de Saint-Exupéry : « pour ce qui est de l'avenir, il ne s'agit pas de le prévoir, mais de le rendre possible ».

Biographie

Le général de corps aérien Vincent Cousin a été nommé secrétaire général adjoint de la défense et de la sécurité nationale le 1er septembre 2021.

Breveté pilote de chasse en 1987, le général Cousin débute sa carrière sur Mirage F1 CR.

Entre 1988 et 1996 il occupe les postes de commandant de l'escadrille « Petit Prince » à l'Escadron de reconnaissance 1/33 « Belfort » (BA 124 Strasbourg) puis de « Charognard » (commandant en second) de la patrouille de France (BA 701 Salon de Provence).

En 1997 il devient leader de la patrouille de France avant de rejoindre, un an plus tard, la BA 128 (Metz) en tant qu'officier d'état-major à la division instruction du Commandement des forces aériennes.

Stagiaire au Collège interarmées de défense en 1999, il devient commandant de l'Escadron de reconnaissance stratégique 1/91 « Gascogne » sur Mirage IV.

S'en suit une carrière en État-major, de 2003 à 2007, en tant qu'officier d'état-major à la division plans, programmes et évaluation (État-major des armées).

De 2007 à 2011, il rejoint Washington (États-Unis). Après un an passé au National War College, il devient attaché de l'air près l'ambassade de France aux États-Unis. Après un retour en France, jusqu'en 2014, en tant qu'adjoint du chef du cabinet militaire du Premier ministre, il retourne aux États-Unis, en tant qu'attaché de défense et chef de la mission défense près l'ambassade de France.

En 2017, il est nommé commandant en second du CDAOA (commandement de la défense aérienne et des opérations aériennes), implanté sur la base aérienne 942 (Lyon). Il en devient le commandant en 2019.

Sa carrière au sein de l'armée de l'air et de l'espace fût marquée par de nombreux déploiements opérationnels. Le général Cousin participa ainsi à l'opération Daguet en Irak (1990-1991), à l'opération Épervier au Tchad (1991), à l'opération Aconit en Irak (1991-1992), à l'opération Crecerelle en ex-Yougoslavie (1992-1993-1994), à l'opération Allied Force au Kosovo (1999), à l'opération Enduring Freedom en Afghanistan (2001-2002) et enfin à l'opération Tarpan en Irak (2003). Il totalise 3 400 heures de vol dont 470 en 164 missions de guerre.

Au cours de sa carrière, le général Cousin fût décoré à plusieurs reprises. Il est ainsi commandeur de la Légion d'honneur et commandeur de l'Ordre national du Mérite. Il a également obtenu la croix de guerre des théâtres d'opérations militaires extérieurs avec l'étoile de bronze, la médaille de l'aéronautique et la croix de la valeur militaire. Son expérience aux États-Unis fût également récompensée puisqu'il fût nommé officier de la légion du mérite. ◂

LE SGDSN SE TRANSFORME

Le projet de transformation numérique du SGDSN

Banc de paramétrage des postes nomades, Tour Mercure.

Contexte et enjeux

Le plan stratégique du SGDSN 2019-2022 fait de la transformation numérique un des chantiers majeurs à conduire en suivant une logique de simplification, de partage et d'efficacité. Les orientations stratégiques suivantes guident les travaux de ce chantier confié depuis 2020 à l'OSIIC :

- planification des projets informatiques centrée sur les besoins « métier » et priorisée dans le cadre d'un schéma directeur traitant aussi bien des projets d'infrastructures techniques que des projets applicatifs « métier » ;
- dématérialisation des documents et des processus ;
- généralisation de l'usage de l'Extranet comme réseau de travail principal, en limitant l'emploi du réseau Intranet aux seuls besoins d'échanges d'informations classifiées ;
- recours privilégié à l'externalisation pour satisfaire les besoins éloignés du cœur de métier de l'OSIIC ;
- amélioration de l'accompagnement des usagers dans leur appropriation des outils et des services mis à leur disposition ;
- meilleur recueil des besoins « métier » exprimés par les différentes directions ;
- développement des services numériques transverses et standardisés, au détriment d'offres spécifiques à chaque « métier ».

État des lieux et feuille de route

L'année 2019 a principalement été consacrée à la réalisation d'un état des lieux de la maturité numérique du SGDSN visant à :

- identifier les forces et faiblesses du SGDSN, tant au niveau des directions métiers que de sa direction du numérique ;
- déterminer les axes de progrès, les besoins et actions prioritaires à conduire ;
- élaborer une feuille de route et estimer les prérequis nécessaires pour la mettre en œuvre.

L'état des lieux a notamment montré la nécessité d'accompagner la sous-direction du numérique de l'ANSSI afin qu'elle soit en mesure de conduire la transformation numérique du SGDSN.
Les recommandations issues de cet état des lieux ont été prises en compte dans la phase de préfiguration à la création de l'OSIIC afin que cette nouvelle entité se dote dès sa création d'une organisation et de moyens adaptés tels que : le renforcement des fonctions dites de gouvernance, la séparation des fonctions d'ingénierie et d'exploitation, l'évolution de la gestion de projet, une meilleure prise en compte des besoins « métier ».
Fin 2020, l'OSIIC a ainsi établi un schéma directeur 2020-2023 intégrant pleinement dans ses objectifs stratégiques la transformation numérique du SGDSN.

Évolution du pilotage de la transformation numérique

Afin de mettre en œuvre les orientations du plan stratégique, un directeur de projet, rattaché au secrétaire général adjoint du SGDSN, a été désigné en 2019 pour piloter la transformation numérique, en lien étroit avec la sous-direction du numérique de l'ANSSI.

La création de l'OSIIC au 1er juillet 2020, reprenant la mission de direction du numérique du SGDSN portée par la SDN de l'ANSSI, a nécessité la mise en place de nouvelles modalités de fonctionnement entre le directeur de projet de transformation numérique, l'OSIIC et les directions métier du SGDSN. Au printemps 2021, il a été décidé de confier intégralement la mission de transformation numérique du SGDSN à l'OSIIC. Le pôle Gouvernance de l'OSIIC est responsable de sa mise en œuvre, de son suivi et de l'atteinte des objectifs.

Le contexte sanitaire de l'année 2020 a imposé un recours très fortement accru au télétravail, et plus généralement à des modalités de travail en « distanciel ».

Renforcement de la « relation client »

Dès sa création, l'OSIIC s'est attaché à clarifier son offre de services numériques et à reconstruire sa relation client. Les résultats de ses travaux se traduisent par :

- l'édition d'un premier catalogue de services internes ;
- une démarche d'amélioration continue de ses processus de gestion des demandes et des incidents ;
- la mise en place d'un réseau de référents « métier » permettant de recenser les besoins prioritaires des « métiers », de les hiérarchiser, d'assurer la bonne diffusion de l'information et d'accompagner le changement ;
- le renforcement de la communication auprès des utilisateurs : messages d'information, *newsletter*, guides, formations.

Ces travaux seront poursuivis en 2021-2022, notamment par la mise en place au sein du SGDSN d'un nouveau portail de communication centralisant l'information et intégrant de nouveaux services numériques unifiés. Enfin, l'OSIIC poursuivra ses efforts de communication, de formation et d'accompagnement au changement auprès des directions « métier ». ▶▶▶

Réponse à la crise sanitaire

Le contexte sanitaire de l'année 2020 a imposé un recours très fortement accru au télétravail, et plus généralement à des modalités de travail en « distanciel », notamment en matière de réunions interservices. Cette adaptation a été tout particulièrement délicate à mener pour un organisme comme le SGDSN, dont les principaux outils de travail reposaient sur des systèmes d'information classifiés, par construction non accessibles à distance.

Après le déploiement massif de terminaux portables (téléphones et ordinateurs) dans les premiers mois de la pandémie, réalisé sur la base d'outils préexistants qui ne répondaient pas nécessairement à toutes les attentes ergonomiques et fonctionnelles des utilisateurs, l'OSIIC a agi en priorité selon deux axes, indispensables à la mise en œuvre efficace et dans la durée de ces nouvelles modalités de travail :

- la généralisation à l'ensemble du SGDSN, en premier lieu, d'un réseau de travail « Extranet », sécurisé, mais non classifié, complémentaire des réseaux classifiés et permettant le traitement d'un certain nombre de missions transverses à distance – cette généralisation était effective fin 2020 ;

- le développement accéléré, dans un second temps, d'une solution de mobilité (ordinateur portable avec VPN « comme au bureau ») plus compatible avec les besoins ergonomiques et fonctionnels exprimés par les utilisateurs – cette solution, entrée en test fin 2020, a été généralisée à l'ensemble des agents du SGDSN en 2021.

Un travail de fond a par ailleurs été engagé afin de transférer des applications métiers non classifiées, mais historiquement hébergées sur des réseaux classifiés, vers le nouveau réseau Extranet, afin de permettre leur mise en œuvre en mobilité. Ce travail, qui se poursuit en 2021, est au demeurant cohérent avec les orientations fixées par la nouvelle instruction générale interministérielle n° 1300, relative au secret de la défense nationale, qui prône une classification au plus juste. Des travaux restent également à mener afin de permettre l'accès à différentes solutions de visioconférence depuis les terminaux mobiles sécurisés du SGDSN, sans rompre le modèle de sécurité de ces derniers. ◄

►►►

Évolution des processus de travail

La transformation numérique a également été initiée sous l'angle de la transformation organisationnelle et de l'évolution des processus de travail. Ce travail sera conduit en 2021 avec la division des moyens généraux du SAG portant des services transverses essentiels au SGDSN (ressources humaines, courrier, reprographie, infrastructure). Cette refonte sera élargie progressivement à d'autres entités du SGDSN, en particulier en raison de la création de nouveaux sites distants et le développement de la mobilité, induisant une importante transformation des habitudes de travail historiques. ◄

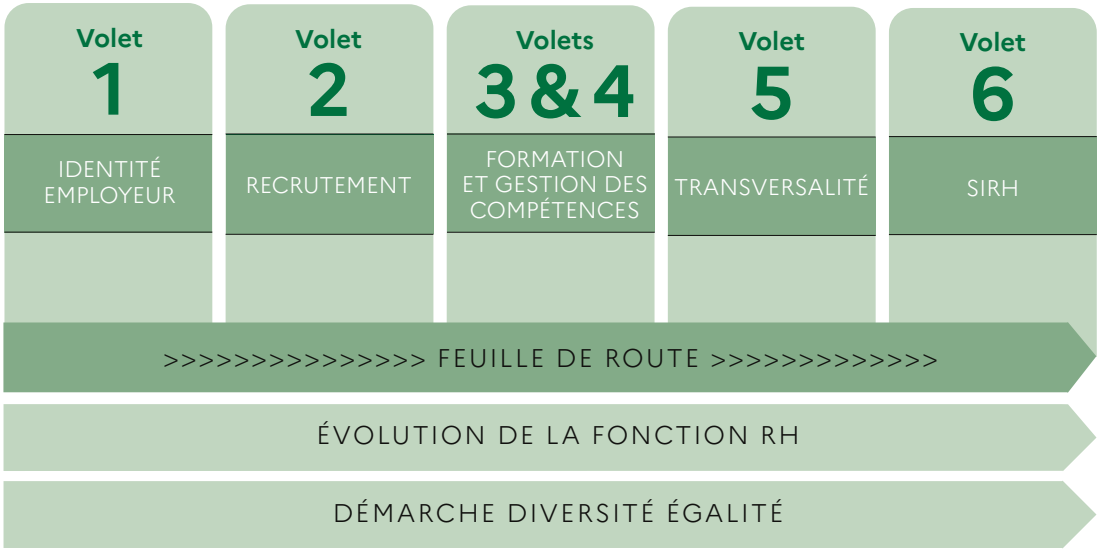
Le projet de transformation RH du SGDSN

Genèse : l'évolution de la structure et des missions du SGDSN

Le projet de transformation RH est l'un des chantiers majeurs concernant le fonctionnement et l'organisation du SGDSN, identifié dans le plan stratégique 2019-2022, au même titre que la transformation numérique. Son lancement a été décidé par la direction du SGDSN ; il touche à la fois au champ des ressources humaines, mais aussi, plus largement, à l'identité de l'institution.

Il est issu d'une réflexion sur l'évolution du SGDSN, notamment l'extension de son champ d'activité et le rattachement d'entités opérationnelles. La forte évolution de ses effectifs (de 353 personnes en 2009 à 1279 au 31 décembre 2020) et les caractéristiques des talents qui y servent nécessitaient de revoir la manière de les recruter et de les gérer.

Projet de tranformation RH



Organisation : une équipe projet transverse et une dynamique participative

Le projet est porté par le secrétaire général et le secrétaire général adjoint, qui président le comité de pilotage du projet.

L'esprit du plan stratégique étant de mettre la réflexion collective au service d'objectifs très opérationnels, les conditions du succès de la transformation RH résident dans la mobilisation des équipes projet, c'est-à-dire les acteurs RH et les personnes qui exercent dans le cœur de métier du SGDSN.

Au lancement du projet, fin 2019, après une phase de diagnostic, il a été choisi de commencer par les méthodes et les outils. À cet effet, une feuille de route co-construite grâce à une dynamique participative associant « métier » RH et *managers* représentant chacune des directions et entités, a été validée en mars 2020.

Cette feuille de route exprime concrètement la volonté des parties prenantes de partager les bonnes pratiques, de se doter de cadres de gestion et d'outils communs, pour mieux valoriser la richesse que constituent les femmes et les hommes qui servent au SGDSN. Elle comprend six volets qui traduisent les priorités dans lesquelles s'investissent les équipes projet.

Priorité 1 : Développer l'identité du SGDSN en tant qu'employeur pour accompagner les évolutions récentes de la maison et attirer autant que fidéliser les talents, notamment dans les métiers en tensions et les compétences rares dont a besoin le SGDSN.

Priorité 2 : accompagner les acteurs vers un recrutement plus efficient (300 recrutements par an au SGDSN)

Priorités 3 : mettre en place une politique de formation

Priorité 4 : valoriser la compétence et développer l'accompagnement des parcours professionnels, car toute affectation au SGDSN est potentiellement un atout dans une carrière et de véritables parcours peuvent désormais s'y réaliser, notamment dans les métiers de la filière numérique et SIC (systèmes d'information et de communication).

Priorité 5 : développer la transversalité RH

Priorité 6 : mettre en place les systèmes d'informations RH adaptés et interopérables

La transformation RH traduit, par ailleurs, l'engagement du SGDSN en faveur de la diversité et de l'égalité professionnelle femmes-hommes, priorité gouvernementale. ▶▶▶

Renforcement de l'identité du SGDSN en tant qu'employeur – Plan d'actions

3 objectifs :

- ▶ améliorer les conditions d'intégration
- ▶ renforcer le sentiment d'appartenance et la cohésion
- ▶ développer la communication interne et élargir la diffusion de l'information RH

▸▸▸

Enjeux : une démarche ambitieuse au service de tous

(agents, managers, gestionnaires RH)

En s'appuyant sur le professionnalisme des gestionnaires RH du SGDSN, le projet de transformation RH a pour ambition de **doter le SGDSN d'une politique adaptée à ses besoins croissants de recrutement, de diversification et de spécialisation.**

Cette démarche inclut plusieurs dimensions, interdépendantes :

- une dimension **stratégique** : *quelles politiques RH pour relever les nouveaux défis du SGDSN ?*
- une dimension **organisationnelle** : *comment adapter la fonction RH aux enjeux et besoins ?*
- une dimension **opérationnelle** : *comment faire évoluer les processus et de quels outils se doter ?*

Réalisations : évolution de la fonction RH, développement de l'identité du SGDSN et conception de politiques RH transversales

La réflexion menée sur l'***organisation*** de la fonction RH a donné lieu à des décisions visant à renforcer le service de l'administration générale (SAG), notamment pour lui donner les moyens de porter ces nouvelles ambitions et de s'adapter à ses nouveaux outils de travail. Ainsi le service de l'administration générale comprendra une sous-direction entièrement consacrée à la gestion des ressources humaines. Elle disposera en son sein d'une fonction de gestion prévisionnelle et développera les politiques RH transversales.

Une enquête a été conduite à l'automne 2020 auprès de l'ensemble du personnel du SGDSN au sujet de l'***identité du SGDSN*** employeur, qui a permis d'établir un plan d'action articulé autour de l'amélioration de l'intégration, du renforcement de la cohésion et du développement de la communication interne. C'est dans ce cadre que le SGDSN a défini les valeurs qui l'animent.

En matière de ***diversité et d'égalité professionnelle entre les femmes et les hommes :***

- des **formations** adaptées au contexte et aux enjeux du SGDSN sont dispensées ;
- une **enquête** en ligne a été menée afin de déterminer les axes de la politique du SGDSN pour lutter contre les discriminations, favoriser la diversité et l'égalité professionnelle entre les femmes et les hommes.

Le parcours RH a été sensiblement amélioré :

- des avancées notables ont été réalisées pour l'accompagnement de la mobilité interne des agents du SGDSN ;
- de nouveaux modèles d'offre d'emploi et de fiche de poste ont été élaborés ;
- le parcours d'accueil et d'intégration des nouveaux arrivants a été amélioré ;
- le livret d'accueil a été refondu ;
- une offre de formation interne au recrutement a été conçue.

S'agissant des ***outils RH***, plusieurs projets sont menés de front par le SAG avec le concours étroit de l'OSIIC, de l'ANSSI et des officiers de sécurité des systèmes d'information. Il a notamment été décidé d'adopter le SI RenoiRH, pour opérer de manière intégrée la gestion administrative et la paie. Le projet débutera en janvier 2022 en vue du déploiement de ce nouveau système début 2023. Dans l'intervalle une optimisation des outils RH actuels est réalisée.

Le développement d'actions de **communication interne**, notamment grâce à la création de nouveaux supports, a créé une réelle synergie pour toutes les dimensions du projet. ◂

51, boulevard de la Tour-Maubourg
75700 Paris Cedex 07 SP
www.sgdsn.gouv.fr