PREMIÈRE
MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

RAPPORT D'ACTIVITÉ 2022

RAPPORT D'ACTIVITÉ 2022

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

Crédits photo :
© SGDSN
© ANSSI
© Pixabay (fancywave, pixelcreatures)
© Ministère de l'économie, des finances et de la souveraineté industrielle et technologique
© Conseil de l'UE
© Freepik (jcomp, mrsiraphol, viarprodesign, DCStudio, janoon028, lifestylementary, fanjianhua, wirestock, rawpixel, svstudioart)

SOMMAIRE

ÉDITO

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

Le présent rapport rend compte de l'activité de l'ensemble du SGDSN durant l'année 2022. À ce titre, il contribue à satisfaire à l'obligation – collective, en l'occurrence – qui incombe à chaque agent public de justifier de l'exécution de ses missions. Du SGDSN, maison des secrets, il n'est pas possible de tout dire. En revanche, il est important d'en dire le plus possible tant sa culture et celle de l'ensemble de ses composantes est le service de l'État, dans le champ de la défense et de la sécurité, ainsi que de la protection de nos concitoyens.

Cette année aura été marquée par la tenue des grandes échéances civiques qui rythment la vie de la République : l'élection présidentielle et les élections législatives. Sous l'égide des garants de l'élection que sont le Conseil constitutionnel, la Commission nationale de contrôle de la campagne en vue de l'élection présidentielle et l'Autorité de régulation de la communication audiovisuelle et numérique, le SGDSN a mis en œuvre un dispositif de protection, armé par l'Agence nationale de sécurité des systèmes d'information dans le domaine de la cybersécurité et par le service de détection et de lutte contre les ingérences étrangères, Viginum. Ce dispositif a été maintenu pour les élections législatives. Il a fonctionné à la satisfaction de ces garants de la sincérité du scrutin.

Au-delà de ces élections, dans l'accomplissement des missions du SGDSN, l'année 2022 aura été particulièrement remplie. Au mois de janvier, la France prenait la présidence du Conseil de l'Union européenne (PFUE) pour un semestre. L'année 2022 a ainsi mobilisé nombre d'entre nous sur l'ensemble des sujets que nous traitons en commun avec les autres États membres et avec les services de l'Union européenne. Rencontres de nos interlocuteurs, animation de groupes de travail, négociations furent ainsi notre quotidien, en lien avec nos collègues du secrétariat général aux affaires européennes et les ministères partenaires. Cet important investissement a porté ses fruits : le bilan de la PFUE est particulièrement positif. Tous les objectifs que nous nous étions fixés ont été atteints. La parution des directives Résilience des entités critiques (REC) et *Network and Information Security 2* (NIS2) le 27 décembre 2022 figure au premier rang des réalisations dont nous pouvons être légitimement fiers. ▶▶▶

ÉDITO

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

Au plan international, le début de l'année 2022 aura été marqué par le déclenchement de la guerre en Ukraine. Notre continent vit ainsi le retour des conflits de haute intensité, avec un impact terrible sur la population civile ukrainienne. Nous savons désormais que grâce au patriotisme et au courage des Ukrainiens, ainsi qu'au soutien des États-Unis et de l'Europe, l'Ukraine résiste victorieusement. Mais le conflit s'allonge et ses conséquences seront durables et profondes.

Cette guerre est suivie de près par le SGDSN : la stratégie militaire, la combinaison des effets dans les champs matériels et immatériels, l'utilisation des moyens dits hybrides, le rôle du renseignement d'intérêt militaire et de la capacité à détecter et exploiter les signaux électromagnétiques, les sanctions économiques et leurs effets, la mobilisation des sociétés civiles pour maintenir l'effort de guerre dans la durée… Bref, la complexité des effets de ce conflit est pour nous une source de réflexions sur notre planification et sur les évolutions de l'entraînement de tous ceux qui doivent participer à la gestion des crises.

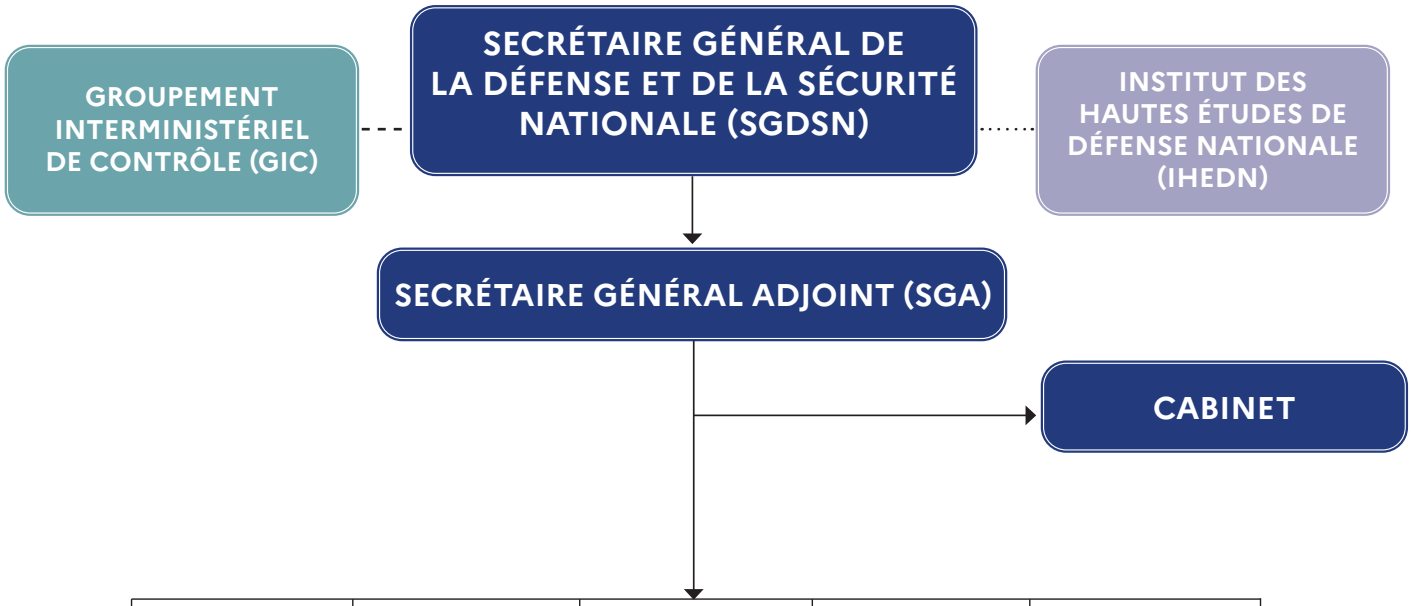
De façon générale, les exercices conduits en 2022 ont permis d'éprouver des scénarios exigeants et réalistes au regard du contexte sécuritaire : risques de cybersécurité, risques énergétiques, préparation des grands événements sportifs de 2023 et 2024 sont autant de sujets qui nous occupent quotidiennement. Parallèlement, la refonte de la planification engagée lors de la crise sanitaire a été menée à bien et achevée en 2022. La nouvelle planification de sécurité nationale offre désormais une approche plus modulaire, comme une boîte à outils toujours plus fournie.

Les conséquences du conflit ont également nourri les travaux que le SGDSN a menés dans le cadre de l'élaboration de la Revue nationale stratégique, en préparation du projet de loi de programmation militaire et qui ont été traités lors de 38 réunions du conseil de défense et de sécurité nationale, dont les modalités de préparation doivent beaucoup aux services assurés par l'Opérateur des systèmes d'information interministériels classifiés.

En 2023, face aux évolutions de nos environnements stratégique, économique, technologique et diplomatique, et face à la succession des crises qui parfois se superposent, le SGDSN continuera de se transformer et d'adapter son organisation aux besoins ; pour cela, son état d'esprit demeurera le même que depuis que figure sur ses murs cette phrase du général de Gaulle : « *servir, au service de tous* ». ◄

ORGANIGRAMME

en date du 26 avril 2023

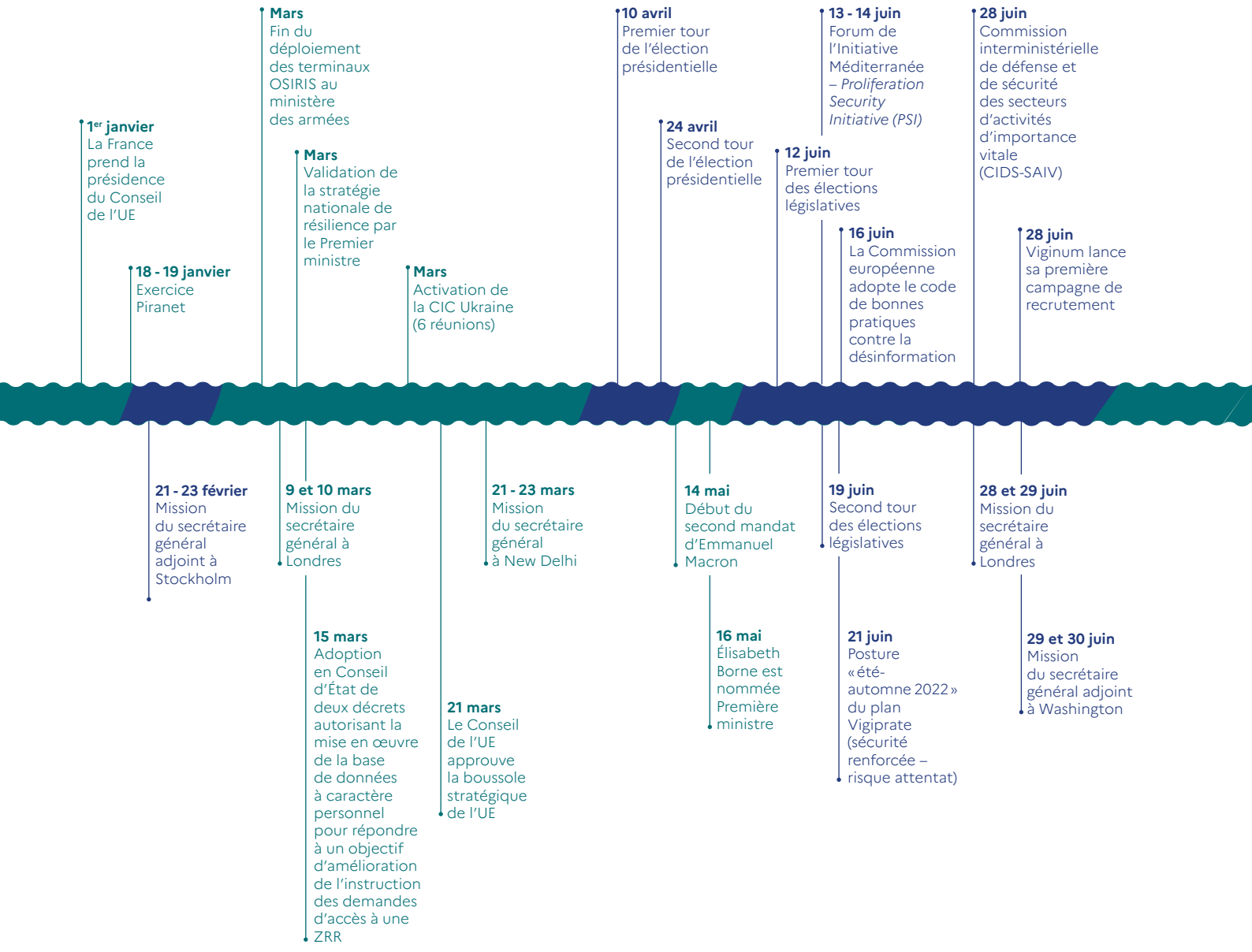


- **Protection et sécurité de l'État (PSE)**
  - Sous-direction planification de sécurité nationale (PSN)
  - Sous-direction protection du secret de la défense (PSD)
- **Affaires internationales, stratégiques et technologiques (AIST)**
  - Sous-direction affaires internationales (AI)
  - Sous-direction non-prolifération, sciences et technologies (PST)
  - Sous-direction exportation de matériels de guerre (EMG)
  - Bureau des affaires spatiales
- **Service de l'administration générale (SAG)**
  - Sous-direction administration générale et finances
  - Sous-direction ressources humaines
  - Détachement de sécurité
- **Agence nationale de sécurité des systèmes d'information (ANSSI)**
  - Sous-direction administration (SDA)
  - Sous-direction expertise (SDE)
  - Sous-direction opérations (SDO)
  - Sous-direction stratégie (SDS)
- **Opérateur des systèmes d'information interministériels classifiés (OSIIC)**
  - Pôle gouvernance
  - Centre de mise en œuvre (CMO)
  - Division ingénierie et innovation numérique (DivIIn)
  - Division exploitation (DivEx)
  - Division opérations (DivOps)
  - Division soutien
- **Service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM)**
  - Division opérations
  - Pôle coordination-stratégie
  - Pôle soutien

Effectifs au 31/12/2022

CAB :	25	ANSSI :	622
PSE :	64	OSIIC :	278
AIST :	57	GIC :	284
SAG :	99	VIGINUM :	43

ÉLÉMENTS DE CHRONOLOGIE 2022

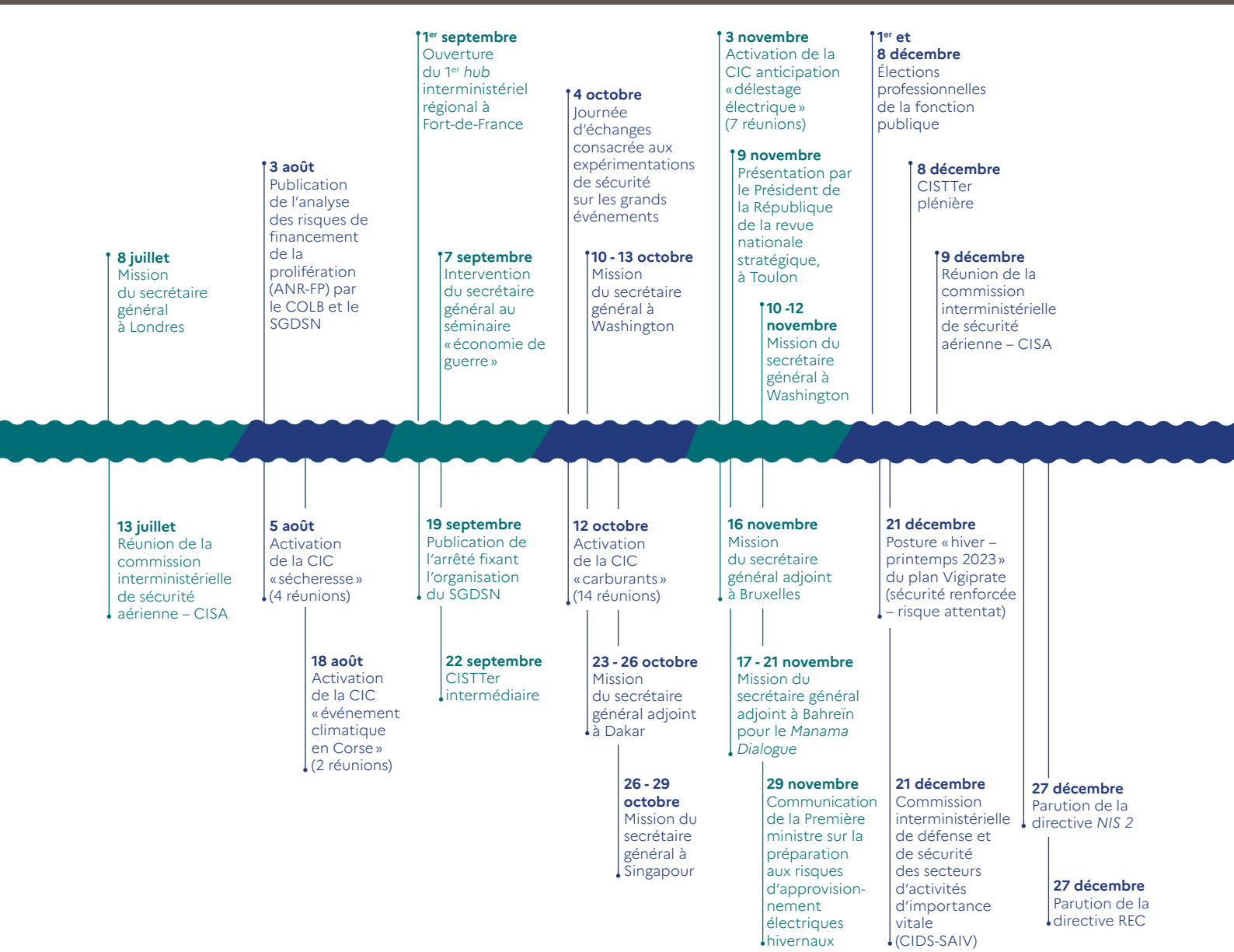


COLMI

7 janvier 2022
1er mars 2022
5 mai 2022
5 septembre 2022
13 octobre 2022

C4

17 janvier 2022
14 février 2022
14 mars 2022
11 avril 2022
16 mai 2022
20 juin 2022
31 août 2022
12 septembre 2022
17 octobre 2022
14 novembre 2022
12 décembre 2022



COLISÉ

9 février 2022
1er avril 2022
8 juin 2022
6 juillet 2022
19 octobre 2022
7 décembre 2022

LES GRANDES MISSIONS DU SGDSN

CONDUIRE LA RÉPONSE AUX CRISES

La réponse de l'État aux crises majeures repose sur une organisation structurée permettant de réagir le plus rapidement et le plus efficacement possible. Cette organisation de gestion de crise implique une claire répartition des responsabilités et des missions, pensée dans une logique de subsidiarité.
Lorsqu'elle affecte plusieurs secteurs ministériels et devient majeure, la crise nécessite une réponse globale de l'État. Dans une telle situation, la Première ministre peut décider d'activer la cellule interministérielle de crise (CIC) afin de mettre en commun l'ensemble des ressources ministérielles en matière de recherche et d'analyse de l'information, d'anticipation, de communication et de décision.

La direction politique et stratégique d'une crise majeure est assurée par la Première ministre, en liaison avec le Président de la République. Les décisions sont prises en conseil de défense et de sécurité nationale, présidé par le Président de la République et dont le secrétariat est assuré par le SGDSN.

Afin de préparer l'État à la gestion d'une situation de crise, les acteurs ministériels peuvent s'appuyer sur une démarche d'anticipation, visant à planifier les actions à conduire. La planification de défense et de sécurité nationale vise à faire face à tous les risques et toutes les menaces susceptibles d'affecter les activités clefs de la vie de la Nation. Coordonnée au niveau interministériel, sur la base d'une stratégie et d'un processus décisionnel commun, elle s'appuie sur les responsabilités de chaque ministère. La planification de défense et de sécurité nationale s'inscrit dans des logiques de prévention, de préparation, de moyens de réponse et de retours d'expérience. ◄

Le plan VIGIPIRATE

Instrument à la disposition du Gouvernement dans la lutte contre le terrorisme, le plan Vigipirate a pour objet de mettre en œuvre des dispositifs de prévention et de protection, gradués en fonction de l'évaluation de la menace terroriste, et de développer une culture de la vigilance dans tous les domaines de la vie de la Nation. Le plan permet également de réagir en cas d'acte terroriste sur le territoire national ou à l'étranger, dès lors que des ressortissants et des intérêts français sont visés. Le plan Vigipirate, révisé tous les six mois, repose sur un système à trois niveaux : vigilance ; sécurité renforcée et urgence attentat. Le SGDSN propose au cabinet de la Première ministre une posture élaborée avec l'ensemble des ministères qui détermine les objectifs de sécurité pour la période considérée. ◄

Professionnaliser les acteurs de la gestion de crise

La professionnalisation des acteurs de la gestion de crise vise à garantir un niveau élevé de performance, de réactivité et de technicité dans le traitement d'une crise majeure. Elle concerne non seulement les acteurs mais également les procédures de travail et les méthodes.

Le SGDSN a ainsi développé un programme de formation, sur la base de travaux interministériels initiés dès 2012 pour établir un référentiel d'activités et de compétences, qui visait initialement les personnels armant la cellule interministérielle de crise (CIC), les centres opérationnels (CO) ministériels et les cellules d'appui thématiques.
Le suivi de ce programme de formation des acteurs de la gestion de crise (PAGC) est sanctionné par l'attribution d'un diplôme universitaire (DU) « gestion interministérielle de crise ». Prenant appui sur ce programme, le SGDSN a proposé en 2021 le développement d'une nouvelle politique de professionnalisation des acteurs de la gestion de crise (PPAGC) élargissant son contenu à tous les niveaux de responsabilité (cabinets ministériels, cadres dirigeants, futurs cadres de haut niveau…). ◄

Adapter les instruments juridiques

Les dispositifs de préparation et de gestion de crise doivent s'appuyer sur des bases juridiques solides.

À cet effet, le SGDSN dispose d'une expertise juridique pour préparer les projets d'accords intergouvernementaux intéressant la sécurité nationale et contribuer aux adaptations législatives et réglementaires, permettant de disposer de nouveaux outils juridiques face aux risques et aux menaces, tout en assurant la concertation interministérielle nécessaire à l'adoption des textes relevant de la compétence de différents départements ministériels.

Le SGDSN contribue en particulier à la rédaction et la mise en œuvre des dispositions législatives et réglementaires dans le cadre de la planification interministérielle de défense et de sécurité nationale et de la protection du secret de la défense nationale. ◄

DÉVELOPPER LA RÉSILIENCE DE L'ÉTAT

Chiffres clés

73
actions réparties
au sein de

3
axes stratégiques

3
déclinaisons de la SNR :
vers les collectivités territoriales,
le monde économique
et les citoyens

Adoption et mise en œuvre de la stratégie nationale de résilience (SNR)

Après une première phase de consultation interministérielle initiée en 2021, la stratégie nationale de résilience (SNR) a été validée par le cabinet de la Première ministre le 21 avril 2022. Cette stratégie, à vocation opérationnelle, vise à offrir une vision complète de l'ensemble des politiques publiques concourant à la résilience de la Nation.

Elle se décline en 73 actions concrètes, réparties autour de trois axes stratégiques : préparer en profondeur l'État aux crises ; développer des moyens humains et matériels pour faire face ; améliorer la communication publique relative aux enjeux de résilience. L'avancement des actions est suivi au sein du Comité interministériel pour la résilience nationale (CIRN), qui a été installé le 1er février 2023 par le directeur de cabinet de la Première ministre.

Au-delà des actions relatives aux missions menées par les services de l'État, y compris au niveau déconcentré, le Gouvernement souhaite décliner la SNR auprès de l'ensemble des forces vives de la Nation, à savoir les collectivités territoriales, les entreprises et les citoyens.

La déclinaison de la SNR auprès des collectivités territoriales a été engagée dès l'été 2022 dans le cadre d'un dialogue avec les principales associations d'élus, afin de les associer aux travaux et identifier des collectivités volontaires. Cette démarche vise à soutenir les initiatives participant au renforcement de la résilience des territoires et à mieux partager les retours d'expérience utiles à l'ensemble des acteurs.

S'agissant des entreprises, l'année 2022 a été l'occasion d'initier une réflexion interministérielle sur la nécessité de constituer des stocks stratégiques et les dispositifs à mettre en œuvre pour faire face à des crises majeures et assurer la continuité de la vie économique de la Nation.

Enfin, les premiers travaux ont été lancés pour faire du citoyen un acteur de la résilience de la Nation, mieux informé sur l'état des risques et les possibilités d'engagement au service de l'intérêt général.

Contribuer à la sécurité des grands événements sportifs 2023 et 2024

En 2022, la direction PSE a intensifié son action au bénéfice des ministères impliqués dans la préparation des grands événements sportifs à venir : coupe du monde de rugby 2023 et jeux Olympiques et Paralympiques de Paris 2024 (JOP24). Elle a ainsi veillé à la cohérence d'ensemble des initiatives de lutte anti-drones (LAD) et de protection NRBC-E, en organisant des expérimentations fondées sur des cas d'usage et en proposant des

évolutions du cadre juridique. Elle a, par ailleurs, poursuivi l'animation d'exercices majeurs et promu la recherche et l'innovation en matière de technologie de sécurité.

LA LUTTE ANTI-DRONES (LAD)

Les travaux interministériels engagés pour conforter la LAD ont été poursuivis : analyse de la menace, évaluation de la vulnérabilité des sites de compétition, identification des besoins en moyens de protection, intégration de ceux-ci et structuration du commandement de ces capacités. En 2022, à l'occasion de deux commissions interministérielles de sûreté aérienne (CISA), il a été rendu compte de l'avancée de ces actions au cabinet de la Première ministre.

La direction a, par ailleurs, piloté en juillet 2022 une expérimentation de moyens de lutte antidrones sur le site olympique du stade Orange Vélodrome de Marseille. Précédée par 18 mois de travaux préparatoires, cette expérimentation de grande ampleur a permis de tester la détection de drones en conditions opérationnelles réelles et en milieu urbain.

Enfin, la direction a contribué financièrement à la réalisation d'un autre important exercice (COUBERTIN LAD) conduit par le ministère des armées en janvier 2023. Avec le concours d'industriels, l'exercice a permis de valider les principes d'intégration interministérielle des moyens existants (interconnexion des systèmes, architecture de commandement, outil de supervision…) et d'identifier les principaux jalons qui mèneront à une pleine capacité opérationnelle avant les JOP24.

LA LUTTE CONTRE LA MENACE NRBC-E

Présidé par le SGDSN, le comité stratégique NRBC-E a permis par deux fois, en 2022, de suivre l'évolution du programme interministériel d'action NRBC-E 2021-2023, du contrat capacitaire interministériel de lutte contre le terrorisme NRBC 2021-2024 et d'effectuer un point d'étape de la préparation des JOP24 dans le domaine NRBC.

La fin de l'année 2022 a, par ailleurs, été marquée par un travail de coordination de la réponse à un appel à projet européen : *RescUE stockpilling NRBC*, placé sous la responsabilité du ministère de la santé et financé par la Commission. La France a été retenue pour 166 millions d'euros d'achat d'équipements NRBC, entreposés en métropole, et qui pourront être mobilisés pour les grands événements. Un second appel à projets européens *RescUE NRBC détection, prélèvements, identification et surveillance* a mobilisé une nouvelle équipe interministérielle avec une demande finale de 75 millions d'euros d'achat adressée à la Commission.

S'agissant de la lutte contre les explosifs, le centre de certification des unités cynotechniques privées pour la recherche d'explosif, dont la création a été lancée par la direction PSE et pilotée dorénavant par la direction générale de la police nationale (DGPN), a ouvert ses portes à Biscarrosse le 1er janvier 2023. Un certain nombre de textes réglementaires préparés en 2022 (décret encadrant les unités déployées par les opérateurs d'événementiels et de sites sensibles, arrêtés fixant les modalités d'intervention et de formation initiale…) ont été publiés au début de l'année 2023. ▶▶▶

LES EXPÉRIMENTATIONS DE TECHNOLOGIES DE SÉCURITÉ

Depuis 2019, la direction PSE pilote des expérimentations de sécurité, en partenariat avec la Coordination nationale pour la sécurité des JOP24 et des grands événements sportifs internationaux (CNSJ), le Comité stratégique de la filière des industries de sécurité (CFS-IS) et des opérateurs comme la Fédération française de tennis, le Paris Saint-Germain et l'Olympique de Marseille. La maîtrise d'ouvrage de ces expérimentations est confiée au pôle de compétitivité SAFE-CLUSTER.

L'année 2022 marque la fin d'un cycle de trois années d'expérimentations de moyens de gestion des flux et de contrôle des accréditations, de protection contre la menace nucléaire et radiologique, de détection des explosifs et de lutte anti-drones.

Le premier thème – gestion des flux et contrôle des accréditations – a été mis en œuvre et évalué durant le tournoi de Roland-Garros en octobre 2020. Les enjeux relatifs aux menaces nucléaires et radiologiques ont pour leur part été évalués dans le cadre des expérimentations conduites au Parc des Princes, en 2021. Le stade Vélodrome a, pour sa part, accueilli en 2021 les expérimentations relatives à la détection des explosifs puis, en 2022, celles consacrées à la lutte contre les drones malveillants.

Pour clore ce cycle de trois années d'expérimentation, la direction a organisé le 4 octobre 2022, au sein de l'Hôtel national des Invalides, une journée de restitution des résultats en présence de plus de 150 participants (services de l'État, industriels, opérateurs, gestionnaires de sites sportifs).

LE PROGRAMME D'EXERCICES

Les 29 et 30 novembre 2022, la direction a organisé l'exercice majeur RUGBY22 qui a inauguré une série de trois exercices spécifiquement dédiés à la préparation des grands événements sportifs.

Ces exercices visent à tester l'organisation de la gestion de crise gouvernementale, le fonctionnement de la cellule interministérielle de crise (CIC) et du nouveau centre national de commandement stratégique (CNCS) mais aussi de tester les plans gouvernementaux.

Deux exercices, l'un sur l'articulation CIC/CNCS (11 et 12 juillet 2023) et un autre intitulé JOP23 (5 et 6 décembre 2023), viendront garantir un haut niveau de préparation.

LES ÉVOLUTIONS DU CADRE JURIDIQUE

La direction a contribué en 2022 à la préparation du projet de loi olympique. Le projet intègre des dispositions directement inspirées du programme d'expérimentations en cours. Il s'agit, à titre expérimental, de rendre possible le test de dispositifs de traitement d'images captées par les caméras de vidéoprotection et par les drones ainsi que l'utilisation de scanners à ondes millimétriques pour l'accès aux manifestations sportives, récréatives ou culturelles de plus de 300 personnes.

Chiffres clés de la préparation à la gestion de crise

4
exercices
(PIRANET ; BLACK-OUT ;
GAZ ; RUGBY)

3
thèmes
(cybersécurité ; énergie ;
grands événements sportifs)

2
promotions INSP sensibilisées
à la gestion de crise

+600
agents formés depuis 2019

Par ailleurs, afin de consolider le cadre juridique de la lutte contre les drones malveillants, un décret relatif au brouillage des drones a été élaboré en 2022 sous l'égide du SGDSN. Ce texte réglementaire fixe la liste des autorités compétentes pour délivrer les autorisations d'utilisation des brouilleurs et définit les modalités qui doivent encadrer la mise en œuvre des opérations de brouillage. Le projet ayant reçu un avis favorable du Conseil d'État, le décret n° 2023-204 relatif au brouillage des aéronefs circulant sans personne à bord a été publié le 28 mars 2023. Parallèlement, à l'initiative du ministère des armées, la loi de programmation militaire votée en 2023 intègre des dispositifs supplémentaires de neutralisation des drones représentant une menace.

Renforcer la résilience européenne et la sécurité des institutions

La direction PSE a été fortement mobilisée au premier semestre 2022, dans le cadre de la présidence française du Conseil de l'Union Européenne (PFUE). Les travaux ont porté sur des sujets de fond comme la résilience ou la sécurité des institutions, des négociations de textes comme la directive REC, mais aussi sur l'organisation d'une réunion d'experts UE-USA-CANADA sur la résilience des infrastructures critiques.

DIRECTIVE RÉSILIENCE DES ENTITÉS CRITIQUES « REC »

Avec l'appui de la Représentation permanente de la France auprès de l'UE et du secrétariat général des affaires européennes (SGAE), la direction a négocié de bout en bout cette directive : d'abord au titre de la position politique et technique de la France, sous présidences portugaise puis slovène, puis au nom du Conseil, en menant sous PFUE l'ensemble des trilogues qui ont permis d'aboutir à un accord politique, après près de 80 réunions sous des formats multiples : 35 réunions techniques avec le Parlement et la Commission, 38 réunions bilatérales et 7 séances plénières avec les États membres. Ces négociations ont été conduites en coopération étroite avec les spécialistes de l'ANSSI en charge de la négociation de la directive *NIS2* qui vise à harmoniser et à renforcer la cybersécurité du marché européen. La directive REC devrait, quant à elle, permettre d'améliorer la résilience collective de l'Union.

La transposition de la directive en droit français doit être achevée avant le 17 octobre 2024. Elle sera l'occasion d'une réforme en profondeur de notre dispositif national de sécurité des activités d'importance vitale (SAIV) pour intégrer pleinement cette logique de résilience et renforcer sa coordination. Cette réforme nationale s'inscrit pleinement dans la *Stratégie nationale de résilience* (SNR), dont la direction PSE coordonne également les travaux.

GROUPE *AD HOC* RÉSILIENCE

La gestion des crises et le renforcement de la résilience constituant une politique transversale majeure pour l'Union, le Conseil européen a appelé au

renforcement de la préparation de l'UE et de sa capacité de réaction face aux crises. À partir des réflexions menées durant la présidence slovène, la présidence française a diffusé à l'ensemble des États membres un questionnaire rédigé par la direction PSE portant sur les principaux aspects de la préparation, de la réponse et de la résilience aux crises aux niveaux national et européen. 26 États membres ont répondu.

Constituant un parangonnage particulièrement détaillé sur les volets gestion de crise, en écho aux travaux conduit parallèlement par la direction sur la SNR, les réponses au questionnaire ont été résumées dans un rapport de la présidence qui présente quinze recommandations et servira de base aux travaux futurs.

SÉCURITÉ DES INSTITUTIONS

Dans ce domaine, l'objectif de la sous-direction en charge de la protection et de la sécurité de la défense nationale a été atteint avec l'adoption de la première opinion formelle par le comité de sécurité du conseil (CSC) sur la proposition de règlement relatif à la sécurité des informations. Ce règlement figure parmi les objectifs du plan sur la sécurité des institutions européennes validé par le Président de la République. Parallèlement, la révision des règles de sécurité du Conseil, qui serviront de référence pour le projet de règlement, a également progressé.

RÉUNION D'EXPERTS UE-USA-CANADA SUR LA RÉSILIENCE DES INFRASTRUCTURES CRITIQUES

Organisée les 1er et 2 juin 2022 à Paris, la 11e réunion d'experts UE-USA-Canada sur la résilience des infrastructures critiques a réuni plus d'une centaine de participants de tous les États membres (à l'exception de Chypre et de la Slovaquie), et des partenaires américains et canadiens. Cette rencontre s'inscrivait dans le cycle des réunions d'experts trilatérales du volet « coopération extérieure » du programme européen de protection des infrastructures critiques (EPCIP), qui se tiennent tous les 12 à 18 mois dans le pays qui assure la présidence du Conseil de l'Union européenne, permettant de favoriser les échanges de bonnes pratiques et la coopération internationale sur la protection et la résilience des infrastructures critiques. L'OCDE a été conviée en tant qu'observatrice de cette édition.

La première journée s'est ainsi organisée autour de plusieurs tables rondes pour évoquer l'ensemble du spectre, de la sécurité à la sûreté, en se focalisant sur les menaces internes auxquelles font face les infrastructures critiques mais aussi les risques liés aux catastrophes naturelles et au changement climatique. Les réflexions en cours sur la résilience de ces infrastructures critiques au Canada, aux États-Unis et au sein de l'UE ont également été exposées, permettant de constater l'existence de synergies entre ces pays et des pistes d'amélioration communes. Enfin, trois projets européens financés dans le cadre du programme Horizon 2020 ont fait l'objet d'une présentation de leurs avancements respectifs par les industriels en charge des projets.

La seconde journée s'est déroulée à l'Observatoire de Paris pour une séquence de travail consacrée à l'espace, avec des présentations sur la protection des infrastructures « sols » des programmes spatiaux européens comme EGNOS et la tenue d'une table ronde sur la dépendance de nombreux secteurs et infrastructures critiques aux signaux de navigation par satellite (GNSS) – temps et positionnement. ◄

Questions à...

Nicolas de Maistre

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

Quel regard portez-vous sur l'activité 2022 de votre direction ?

Vu de PSE, une crise chasse l'autre. Dégagés de la crise COVID-19 nous avons contribué à la gestion des crises liées à l'accueil des réfugiés afghans et ukrainiens, au délestage électrique ou aux pénuries d'hydrocarbures. La direction a donc conservé en 2022 un rythme très opérationnel.

Nous avons poursuivi les importants travaux de réforme de la planification (création de l'outil informatique de suivi des plans gouvernementaux ATHENA, nouvelle directive générale interministérielle relative à la planification de défense et de sécurité nationale, réforme du plan nucléaire...) et de mise en œuvre pratique de l'IGI 1300 (création d'une certification des officiers de sécurité, diffusion des outils pédagogiques, négociation des accords généraux de sécurité...). J'ai aussi souhaité, en plus du travail réglementaire habituel, que nous nous assurions de la portée réelle des politiques publiques que nous promouvons. Une attention particulière a ainsi été apportée à la façon dont les acteurs de terrain se saisissent de la planification nationale de crise. J'ai aussi été attentif à la concrétisation de la stratégie nationale de résilience ou encore à la mise en œuvre effective de la protection du secret de la défense nationale.

Par ailleurs nous assurons désormais le secrétariat de trois nouvelles commissions interministérielles, créées au cours de l'année 2022 : une consacrée à la continuité du travail gouvernemental ; une qui traite des questions d'explosifs et une troisième portant sur la résilience nationale. Enfin, les agents de la direction ont été mobilisés par la reprise de nos missions internationales, après deux ans d'interruption. Nous avons notamment participé à la négociation sous présidence française de la directive relative à la résilience des entités critiques (REC) et à l'accueil en fin d'année du comité résilience de l'OTAN, ex-comité des plans civils. Encore une année bien remplie, en somme !

Pourriez-vous préciser les grandes lignes de votre action en 2022 dans les domaines de la gestion des risques et la préparation des grands événements sportifs qui s'annoncent (coupe du monde de rugby et jeux Olympiques et Paralympiques 2024) ?

Nous avons achevé les travaux interministériels visant à refondre le corpus doctrinal relatif à la planification de défense et de sécurité. Initiée au printemps 2021, la nouvelle directive générale interministérielle (DGI) relative à la planification de défense et de sécurité nationale a été signée par la Première ministre au mois de janvier 2023. Il s'agit notamment d'optimiser et de rationaliser les plans nationaux existants dans une approche désormais « tous risques » tout en promouvant une culture de l'anticipation.

La démarche a été complétée par le développement, avec le concours résolu de l'OSIIC, de l'outil numérique ATHENA, visant à permettre une meilleure appréhension de la planification de sécurité nationale par l'ensemble des ministères. Fin 2022, le premier démonstrateur était opérationnel et nous avons débuté l'intégration des fiches mesures de plans, notamment VIGIPIRATE. ATHENA sera déployée par la suite dans les ministères et jusqu'à l'échelon préfectoral.
Par ailleurs, alors que nous organisons d'ordinaire deux exercices majeurs de gestion de crise par an, en 2022 ce ne sont pas moins de quatre exercices qui ont rassemblé l'ensemble des ministères sur des thèmes d'actualité : cybercrises, en lien avec l'ANSSI ; gestion d'un *blackout* électrique généralisé ; hors programmation et à la demande du cabinet de la Première ministre, la capacité de réponse à une situation de tension sur le système gazier ; enfin, en vue de la prochaine coupe du monde de rugby, la gestion d'un grand événement sportif international.

Nous poursuivons aussi notre démarche de professionnalisation des acteurs de la gestion de crise. Le vivier atteint aujourd'hui 600 personnes formées, avec en 2022 de nouveaux modules à destination des futurs hauts fonctionnaires de l'Institut national du service public (INSP) et du Cycle des hautes études de service public (CHESP).

Enfin, je terminerai par le champ des expérimentations que nous pilotons depuis 2019. En effet ces échéances sont des jalons importants susceptibles d'accélérer le recours à de nouvelles technologies au bénéfice de la sécurité et l'occasion de faire valoir les savoir-faire français.

Sur ce dernier volet, pourriez-vous préciser ce que recouvrent concrètement ces expérimentations ?

Notre ambition est de développer des feuilles de route capacitaires dont les jalons sont liés à ces deux grands événements sportifs internationaux. Quatre domaines d'activité qui entrent dans le champ de compétence de la direction sont concernés : la protection des espaces publics, la lutte contre les menaces constituées par les explosifs, la lutte contre la menace NRBC et la lutte anti-drones. À mon sens, les deux défis majeurs sont, d'une part, d'agréger ces solutions au profit des forces de sécurité, en définissant notamment les concepts d'emploi, et, d'autre part, de lever les freins qui limitent, voir interdisent parfois, leur emploi à ce jour.

Sur cette base, en partenariat avec la coordination nationale pour la sécurité des jeux Olympiques et Paralympiques 2024 (CNSJ) et le Comité stratégique de la filière industrielle de sécurité (CFS-IS) nous avons lancé dès 2019 un programme d'expérimentations permettant de tester des solutions en conditions opérationnelles : lors du tournoi de Roland-Garros en 2020 (pour la gestion des flux et des droits d'accès) ; au stade Vélodrome de Marseille et au Parc des Princes en 2021 (notamment sur la détection des armes et explosifs et les enjeux relatifs aux menaces nucléaires et radiologiques) ; et à nouveau au stade Vélodrome de Marseille en 2022 pour tester en conditions réelles des dispositifs de lutte contre les drones malveillants, avec le concours du Centre d'initiation et de formation des équipages drones (CIFED) de l'armée de l'air et de l'espace et de la préfecture de police des Bouches-du-Rhône.

Après près de trois ans d'expérimentations, la direction a animé une journée de restitution et d'échanges le 4 octobre 2022, au sein de l'Hôtel national des Invalides, à destination des acteurs étatiques, des industriels, des opérateurs et gestionnaires de sites sportifs. ◄

SAUVEGARDER LES INTÉRÊTS DE LA NATION

Dialogue stratégique franco-américain sur le commerce de défense

Le SGDSN a participé activement au lancement et à la déclinaison du nouveau dialogue stratégique franco-américain sur le commerce de défense annoncé par les deux présidents en marge du G20 en octobre 2021. Ce dialogue constitue un forum privilégié pour le renforcement de la coopération bilatérale de défense et doit permettre notamment d'aborder des sujets d'intérêt commun dans le domaine du contrôle des exportations de matériels de guerre. Dans le cadre de ces travaux, le SGDSN pilote le sous-groupe consacré aux audits ITAR et EAR menés par les autorités américaines au sein d'entreprises et d'universités françaises.

En 2022, ce sous-groupe s'est réuni à deux reprises, en juin et en octobre. Il a abouti, en particulier, à la définition d'un cadre agréé par la partie américaine pour mener ces audits en France, ainsi qu'à l'organisation par les États-Unis de séances de sensibilisation des entreprises françaises à la réglementation ITAR, avec un premier événement tenu en marge du salon Eurosatory. Ce forum a pour vocation d'étendre éventuellement ce dialogue à d'autres sujets intéressant le contrôle des exportations.◄

Anticipation stratégique

Le SGDSN est chargé d'animer au niveau interministériel la fonction d'anticipation stratégique dans le domaine de la défense et de la sécurité nationale. Cette démarche participe au renforcement de la résilience de la Nation car elle contribue à comprendre ce qui peut précipiter les crises, à en atténuer les effets lorsqu'elles surviennent et à favoriser un retour plus rapide à la normale. La mise en place d'un réseau spécifique au sein des ministères, le renforcement du lien avec les chercheurs et le monde académique et les travaux du comité interministériel d'anticipation (CIA) mis en place en 2021 ont été confortés par la création d'une structure spécifique au sein du SGDSN. Le CIA s'est réuni deux fois en format plénier en 2022 et a permis de finaliser cinq études majeures. Cinq autres études ont déjà été lancées pour 2023. Leurs travaux sont pilotés au sein de groupes de travail interministériels. Une étude a notamment permis d'alimenter les scénarios d'un exercice de crise interministériel.

Menaces hybrides

Les tensions internationales accrues ont contribué à une prise de conscience de l'essor des menaces hybrides. La lutte contre ces menaces protéiformes fait partie des dix objectifs de la revue nationale stratégique (RNS) présentée par le Président de la République à Toulon le 9 novembre 2022. Les travaux interministériels dans ces domaines sont animés par le SGDSN dans le cadre d'un groupe de travail permanent qui s'est réuni quatre fois en 2022. Ils ont permis d'évaluer l'impact en matière hybride du conflit en Ukraine. Cette capacité du SGDSN en fait un pôle d'excellence reconnu et l'interlocuteur privilégié de nos alliés sur ce sujet, aussi bien dans les formats multilatéraux (notamment centre d'excellence d'Helsinki sur les menaces hybrides, groupe horizontal du conseil de l'Union Européenne sur les menaces hybrides) que bilatéraux. En 2022, 15 déplacements internationaux, 17 entretiens bilatéraux et 9 conférences ont été réalisés. Enfin, en 2022, le SGDSN a appuyé l'« équipe France » lors des négociations sous présidence française de l'Union européenne (PFUE) dans le champ hybride, et a organisé dans ce cadre une journée de travail réunissant les correspondants nationaux de l'Union européenne pour la lutte contre les menaces hybrides, en collaboration avec la cellule de fusion hybride du centre de situation et du renseignement de l'UE.

Action internationale

Le positionnement du SGDSN, auprès des très hautes autorités politiques, et sa vision globale issue du travail interministériel, en font un interlocuteur privilégié pour nos partenaires, notamment lorsqu'ils sont dotés d'une organisation comparable à la nôtre (*National Security Advisor* ou *National Security Council*, par exemple) et souhaitent aborder les questions de sécurité au sein des instances multinationales (UE, OTAN), de formats particuliers de dialogue (Inde, Qatar, Singapour notamment) ainsi que dans différents *fora* (Forum de Dakar, *Shangri-La dialogue*, *Manama dialogue*…). Le SGDSN concourt également au rôle que la France, nation résidente de l'Indopacifique par ses territoires ultramarins, entend jouer dans cet espace. Il copilote ainsi avec le ministère de l'Europe et des affaires étrangères la stratégie de notre pays dans la zone et cherche à y valoriser l'engagement accru de l'Union Européenne.

Contre-espionnage académique, technologique et sécurité économique

Les laboratoires de recherche et entreprises innovantes françaises sont des cibles de choix pour les puissances étrangères, aussi bien lorsque ces dernières cherchent à rattraper leur retard technologique que lorsqu'elles se soucient de conserver leur avance. La prévention des captations et/ou détournements des savoirs, savoir-faire et technologies sensibles à des fins de prolifération d'armes de destruction massive, de renforcement d'arsenaux militaires étrangers, de préparation d'actes de terrorisme ou de guerre économique est une priorité nationale. Les menaces associées sont quotidiennes, bien que souvent dissimulées. Afin de s'en prémunir, le SGDSN pilote le dispositif de protection du potentiel scientifique et technique de la Nation (PPST) et a poursuivi en 2022 des travaux réglementaires visant à le renforcer. Le dispositif de la PPST est pensé pour fournir le juste besoin de protection tout en permettant les échanges académiques indispensables à la vitalité de la recherche. Par ailleurs, le SGDSN préside le comité de liaison en matière de sécurité économique, dont le référentiel d'analyse a été utilement renforcé et mis à jour en 2022, permettant de prioriser l'action de l'État sur tout le territoire. ▶▶▶

Lutte contre le financement de la prolifération et du terrorisme

En 2022, le SGDSN a continué de jouer un rôle de premier plan dans la lutte contre le financement de la prolifération et le financement du terrorisme.

Ainsi, le groupe de travail sur le gel des avoirs à but antiterroriste (GABAT), dont le SGDSN assure, avec la CNRLT, le secrétariat exécutif, a confirmé en 2022 son rôle central en matière de lutte contre le financement du terrorisme. Au 31 décembre 2022, 539 mesures de gel des avoirs pour motif de terrorisme étaient en vigueur sur le territoire national.

Le GABAT implique l'ensemble des services et des ministères compétents, s'assure de la bonne circulation de l'information, organise et rend compte des séances de travail. Il simplifie ainsi le recours au mécanisme des gels d'avoirs visant la menace terroriste, qui ont été multipliés par 10 depuis la création du groupe en 2017.

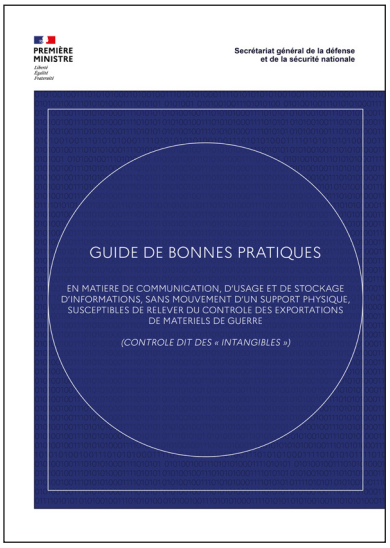
S'agissant du financement de la prolifération, conformément aux recommandations du Groupe d'Action Financière (GAFI), auxquelles la France a contribué activement, un effort particulier a été consacré en 2022 à l'évaluation des risques : le Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB) et le SGDSN ont publié en août 2022 une analyse nationale des risques dédiée à la lutte contre le financement de la prolifération des armes de destruction massive (ANR-FP).

Premier document public en la matière, l'ANR-FP constitue une aide pour le secteur privé, placé en première ligne. Il établit ainsi qu'en France, les vulnérabilités résiduelles sont évaluées à un niveau modéré dans la plupart des secteurs économiques et financiers. ◀

Guide de bonnes pratiques sur le transfert de flux dits « intangibles »

Le SGDSN a coordonné, en concertation étroite avec l'industrie, la rédaction d'un guide de bonnes pratiques en matière de flux « intangibles », comme une documentation transmise par voie dématérialisée. Ce document vise, dans un contexte de recours accru aux technologies de l'information, à améliorer la maîtrise, par les exportateurs, des risques spécifiques liés aux données contrôlées qu'ils sont amenés à stocker, manipuler ou transférer par voie numérique. Il permet de clarifier l'état du droit existant et de préciser les attentes de l'administration afin d'encadrer ces risques et de prévenir l'exportation sans autorisation.

Ce guide, publié en 2023, donnera lieu à une phase de mise en œuvre provisoire, dont le retour d'expérience permettra de l'enrichir. ◄



Exportations de matériels de guerre (EMG) et de biens à double usage (BDU)

Le SGDSN assure le contrôle des exportations de matériels de guerre et préside à ce titre la Commission interministérielle pour l'étude et l'exportation des matériels de guerre (CIEEMG). Les matériels de guerre étant soumis à un régime de prohibition, leur exportation est interdite sans autorisation. En France, ces autorisations prennent la forme de licences d'exportation, dont l'octroi, après avis de la CIEEMG, relève de la Première ministre et du SGDSN par délégation. La CIEEMG a instruit 8 200 demandes en 2022. Près de la moitié de ces demandes portent sur des modifications ou des prorogations de licences existantes. Il s'agit d'une augmentation sensible du nombre des licences délivrées, puisque le cap des 8 000 licences par an a été franchi pour la première fois. Une session plénière de la CIEEMG est organisée par le SGDSN chaque mois, afin de débattre des dossiers sensibles ou qui appellent un examen plus approfondi entre les membres de la commission. Par ailleurs, le SGDSN anime certains travaux interministériels et internationaux relatifs à l'élaboration ou à la modification de politiques d'exportation de matériels de guerre. Le SGDSN est aussi impliqué dans l'instruction de travaux réglementaires dans ce domaine. En 2022, ces travaux ont notamment porté sur la finalisation d'un guide sur les exportations de matériels de guerre dits « intangibles », à paraître en 2023 (*cf.* encadré) ou encore la réforme du processus d'instruction des autorisations de transit des matériels de guerre, entérinée par un décret du 17 juin 2022.

En tant que membre de la Commission interministérielle des biens à double usage (CIBDU), le SGDSN contribue également au contrôle des exportations de biens et technologies à finalité duale. Ce contrôle repose sur le règlement européen 2021/821 entré en vigueur le 9 septembre 2021. Ce règlement prend davantage en compte la question sensible des biens dits de cybersurveillance. Il permet notamment de soumettre à contrôle davantage de matériels et de technologies, par l'intermédiaire d'une clause dite « attrape-tout », en cas de violation des droits de l'Homme. Enfin, il accroît les obligations de transparence des États membres, vise à mieux prendre en compte la question des flux dits « intangibles », et ambitionne une meilleure harmonisation des systèmes de contrôle européens des biens à double usage. Près de 3 800 demandes de licences individuelles ont été

examinées sur l'année 2022. La crise ukrainienne, qui a fortement réduit les exportations de biens sensibles vers la Russie, a conduit le SGDSN à participer activement aux travaux d'élaboration et de mise à jour des sanctions.

Participer à la sécurité dans le domaine spatial

En 2022, le SGDSN s'est transformé en créant un bureau des affaires spatiales pour être en mesure d'accompagner la montée en puissance d'un domaine aux enjeux croissants, que ce soit au niveau de l'Union européenne avec la finalisation du règlement sur la nouvelle constellation Connectivité, les travaux liés au conseil ministériel de l'ESA ou encore les problématiques liées à la suspension des lancements de fusées Soyouz depuis le centre spatial guyanais ou au retard du programme Ariane 6. Ces travaux nécessitent une forte coordination avec les ministères, l'Union européenne et les représentants d'autres États.

En tant qu'autorité nationale responsable de la sécurité du signal protégé (*Public regulated service*) offert par le système de radionavigation par satellites issu du programme européen Galileo, le SGDSN a poursuivi les activités d'instruction des demandes d'autorisation des industriels à travailler sur ce signal.

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

Enfin, le SGDSN a également participé au renforcement de la coopération franco-américaine en co-présidant le premier *Comprehensive Space Dialogue* qui s'est tenu à Paris en novembre et en préparant d'autres dialogues pour 2023. ◄

Questions à...

Charles Touboul

Directeur des affaires internationales, stratégiques et technologiques (AIST)

L'invasion de l'Ukraine par la Russie marque-t-elle une évolution de la conflictualité, et comment la France s'y adapte-t-elle ?

L'invasion de l'Ukraine le 24 février 2022 implique une lecture nouvelle de la géopolitique mondiale, que reflètent par exemple les prises de position lors des votes à l'ONU. L'ordre multilatéral basé sur le droit et sur l'architecture de sécurité européenne est fragilisé. La compétition stratégique se durcit, basculant même dans la confrontation ouverte, avec un recours accru à une combinaison de modes d'actions militaires et non militaires, à la manipulation de l'information, voire à la menace nucléaire à fins d'intimidation. Cette évolution nécessite une adaptation de notre outil de défense. La prise en compte de la résurgence sur le sol européen du risque de conflit de haute intensité et de l'emploi de stratégies hybrides a guidé les réflexions de la revue nationale stratégique (RNS). Afin de préparer l'État, la population et les forces armées à ce contexte international dégradé, la révision de la loi de programmation militaire s'appuie sur les dix objectifs stratégiques de cette RNS. La direction AIST a été particulièrement impliquée dans l'élaboration de cette nouvelle doctrine et dans la mise en œuvre d'un certain nombre de ses objectifs, tels que la capacité à se défendre et à agir dans les champs hybrides ou encore le développement d'une économie concourant à l'esprit de défense.

Pourquoi avoir créé un bureau des affaires spatiales au sein d'AIST ?

La décision de créer ce bureau au sein du SGDSN répond à un contexte de forte évolution des activités spatiales : le progrès technologique s'accélère, avec des applications civiles comme militaires, de nouveaux acteurs – étatiques ou privés – font leur apparition dans le cadre du *New Space*, et la compétition stratégique, mais aussi industrielle et commerciale, s'intensifie. Face à ces défis, une action coordonnée de l'État est nécessaire pour soutenir les programmes spatiaux qui permettront à l'Europe de disposer d'une autonomie stratégique (Galileo, GovtSatCom, Connectivité, futur Copernicus), pour préserver notre souveraineté en matière d'accès à l'espace, ou encore pour renforcer la résilience de nos infrastructures spatiales face à des agressions de toutes natures. Traiter l'ensemble de ces problématiques qui impliquent un grand nombre d'administrations nécessite une coordination interministérielle soutenue. La place occupée par les questions de défense et de sécurité nationale a également contribué à confier au SGDSN la responsabilité de coordonner l'ensemble des parties prenantes.

Enfin, les dialogues spatiaux que le SGDSN anime ou co-anime avec plusieurs grands partenaires (États-Unis, Japon, Inde) se multiplient et s'intensifient.

Sur toutes ces questions par nature transversales, le bureau travaille en lien étroit avec les autres composantes de la direction AIST, les autres directions du SGDSN, et en particulier les équipes de PSE et de l'ANSSI, ainsi qu'avec de nombreux ministères et opérateurs. ◄

RENFORCER LES CAPACITÉS DE PROTECTION ET DE RÉPONSE À LA CYBERMENACE

Une menace croissante

Les observations de l'Agence nationale de sécurité des systèmes d'information (ANSSI) font apparaître que, malgré une année marquée par le conflit russo-ukrainien et ses effets dans le cyberespace, les tendances identifiées en 2021 se sont confirmées en 2022.

Le niveau général de la cybermenace se maintient avec 831 intrusions avérées contre 1082 en 2021. Cette légère diminution ne saurait être interprétée comme une baisse du niveau de la menace. En effet, la diminution de l'activité de cyber-rançonnage des opérateurs régulés publics et privés observée par l'ANSSI traduit avant tout une bascule d'effort des attaquants. Les activités criminelles visent désormais prioritairement des entités moins bien protégées. Parallèlement les malfaiteurs améliorent constamment leurs capacités d'attaque, utilisées à des fins crapuleuses, d'espionnage et de déstabilisation.

Cette amélioration s'illustre en particulier dans le ciblage des équipements périphériques pour installer des accès plus discrets et pérennes aux réseaux des victimes. Ce ciblage périphérique se décline également dans le type d'entités attaquées et confirme l'intérêt des attaquants pour les prestataires, les fournisseurs, les sous-traitants, les organismes de tutelle et l'écosystème large de leurs cibles finales.

La convergence des outils et des techniques des différents types d'attaquants s'est poursuivie en 2022 et continue de poser des difficultés de caractérisation de la menace. L'utilisation de rançongiciels d'origine crapuleuse par des services gouvernementaux illustre une porosité déjà identifiée en 2021.

Dans ce contexte difficile, il convient de maintenir ou intensifier l'ensemble des efforts de rehaussement du niveau de cybersécurité des entités publiques, parmi lesquelles les collectivités et les établissements hospitaliers. S'agissant de ceux-ci, un important travail est en cours, à la demande de la Première ministre, sous l'égide du ministre de la santé et avec le concours de l'ANSSI.

Consolider l'écosystème

En 2022, l'ANSSI a continué d'œuvrer à la montée en puissance du niveau de cybersécurité général et à la mobilisation d'un écosystème en pleine construction.

La mise en place du plan France Relance s'est poursuivie et accélérée en 2022, avec au bilan l'accompagnement

de 950 établissements publics et de 11 000 communes. Cet accompagnement s'est décliné autour de trois axes :
▶ aider des entités à initier un parcours de cybersécurité ;
▶ appuyer le développement de centres de réponse aux cyber-incidents (CSIRT) régionaux ;
▶ favoriser, au travers d'appel à projets, la mutualisation d'un certain nombre d'outils.
Dans cette perspective, des efforts ont été entrepris afin de renforcer les capacités de réponse du secteur privé, avec notamment la création de 12 CSIRT régionaux incubés par l'ANSSI, 5 CSIRT sectoriels accompagnés et 10 CSIRT ministériels en cours de construction. Par ailleurs, la France a pris en 2022 la présidence du réseau européen CSIRT *Network* pour 18 mois. L'InterCERT France, première association de CSIRT en France, se renforce également avec l'entrée de 24 membres, portant à près de 80 le nombre total de membres, et la création de 2 communautés sectorielles de CERT (énergie et défense).

Une PFUE fructueuse

En 2022, année de présidence française du Conseil de l'Union européenne (PFUE), l'ANSSI a encore intensifié son engagement européen.
La PFUE s'est achevée sur la validation de l'ensemble des objectifs fixés dans son ambitieux programme en matière de cybersécurité.

L'exercice *Cybersecurity Crisis Liaison Exercise on Solidarity* (EU-CyCLEs), conduit en février 2022 et coorganisé avec le Service européen pour l'action extérieure et l'Agence de l'Union européenne pour la cybersécurité (ENISA), a été un succès. Il a permis la mise en situation – à distance – du réseau européen des acteurs de la gestion de crise cyber CyCLONe (*Cyber Crisis Liaison Organisations Network*). Cet exercice a ainsi contribué à mieux articuler dans l'avenir les deux composantes de la communauté des acteurs de la gestion de crise : les spécialistes en charge des aspects techniques et les diplomates. À l'issue, le Conseil, dans ses conclusions, a repris à son compte les travaux promus par l'ANSSI, sur la mise en place d'une posture européenne de cybersécurité. En plus de sa fonction de sensibilisation en matière de cybersécurité, cet exercice a permis d'illustrer et promouvoir une vision française de la gestion des crises de cybersécurité, notamment sur le rôle indispensable du secteur privé « de confiance » comme démultiplicateur des capacités publiques.

L'adoption par les États membres, le 22 juin 2022, du compromis élaboré en trilogue politique avec le Parlement européen sur la directive *NIS2* a atteint l'objectif législatif de concrétisation des négociations sous présidence

Le rapport d'activité 2022 de l'ANSSI a été publié le 25 avril 2023. Il est disponible sur le site internet de l'Agence.

française. Le texte traduit l'ambition initiale d'un renforcement massif de la cybersécurité des acteurs économiques et des administrations au sein de l'UE. Il représente un véritable succès pour la PFUE.

Les efforts de mobilisation de l'agence ont enfin été récompensés par la publication, au mois de mars, et l'adoption d'une position commune des États membres, en décembre, sur la proposition de règlement sur la cybersécurité des institutions, organes et agences de l'UE, véritable pendant de la directive *NIS*. ◄

Chiffres clés

Les opérations

2 173
signalements

831
incidents

3
incidents majeurs*

16
opérations de cyberdéfense

*L'évolution du nombre d'incidents majeurs et d'opérations de cyberdéfense n'est pas une mesure de l'évolution de la menace. Elle résulte des différents modes d'engagement des équipes de l'ANSSI qui s'appuie également sur un ensemble de prestataires qualifiés.

Les publications

12
avis techniques publiés

10
guides techniques publiés

8
publication de logiciels en open source

Les qualifications et certifications

155
qualifications et

91
certifications ont été délivrées par l'ANSSI en 2022

La formation

20
formations distinctes

1 557
personnes formées en

62
sessions MOOC :

306 101
utilisateurs inscrits ;

68 635
attestations émises

27
nouvelles formations tierces labellisées

Questions à...

Vincent Strubel

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

Vous avez pris vos fonctions de directeur général de l'ANSSI en début d'année, après avoir occupé le poste de directeur de l'OSIIC. Comment avez-vous perçu l'année 2022 de l'ANSSI depuis l'extérieur ?

Face à une cybermenace qui s'accroît, l'ANSSI a entamé d'importants travaux à la fois pour accompagner l'élargissement de son périmètre d'intervention et pour renforcer la coordination et la coopération avec l'écosystème de cybersécurité. L'année 2022 a été très importante pour l'agence et a été marquée par un certain nombre de réalisations notables.

Dans le cadre de la présidence française du Conseil de l'Union européenne, l'ANSSI a mené à bien les négociations autour de la directive *NIS2*, aboutissant à un texte ambitieux et exigeant pour l'écosystème français et européen. Cette présidence a également été l'occasion de renforcer ses liens avec ses homologues européens au travers notamment du réseau CyCLONe *(Cyber Crisis Liaison Organisation Network)*.

Au niveau national, l'agence a conforté son rapprochement avec l'écosystème. Cela s'est traduit par l'installation de

sa division Industrie et Technologies au Campus Cyber. De plus, les travaux de son antenne à Rennes se sont achevés et des équipes issues des sous-directions Opérations et Expertise pourront s'installer sur le nouveau site à brève échéance désormais.

Sur le plan de la prévention et de la formation, l'agence a consolidé ses rendez-vous annuels, que ce soit par la publication de son *Panorama de la cybermenace 2022* ou en proposant des études toujours plus poussées, telles que son *Observatoire des métiers de la cybersécurité*.

Enfin, comme de nombreux acteurs du SGDSN, j'ai suivi de près les travaux autour de la Revue nationale stratégique, à laquelle l'ANSSI a contribué de manière significative.

Les ambitions affichées dans cette revue pour maintenir la France au premier rang des nations en matière de cyberprotection orienteront l'agence pour les années à venir.

Y a-t-il un projet qui a attiré votre attention dès votre arrivée à l'agence ?

C'est une question difficile… Tous, évidemment !

Cependant, les travaux menés dans le cadre du plan de relance « France 2030 », en raison de leur ampleur, ont un rôle éminemment structurant dans l'élévation du niveau de cybersécurité de notre pays, notamment pour les opérateurs économiques et les collectivités territoriales. C'est aussi le cas pour les établissements de santé qui demeurent en première ligne face à la cybercriminalité, comme la Première ministre le rappelle régulièrement. Ce plan de relance est un formidable outil et j'attache une attention toute particulière à sa déclinaison.

D'ailleurs, la multiplication des parcours de cybersécurité à destination d'acteurs variés, mais toujours d'importance vitale pour le quotidien des Français, associée à la mise en place de centres de réponse aux cyberincidents (*CSIRT*) dans 12 régions métropolitaines et de trois centres de ressources cyber en outre-mer, constitue une avancée majeure qui répond largement aux objectifs que l'agence s'était initialement fixés dans le cadre de ce plan.

Je souhaite que nous prolongions cette dynamique sectorielle et territoriale, désormais éprouvée par l'expérience.

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

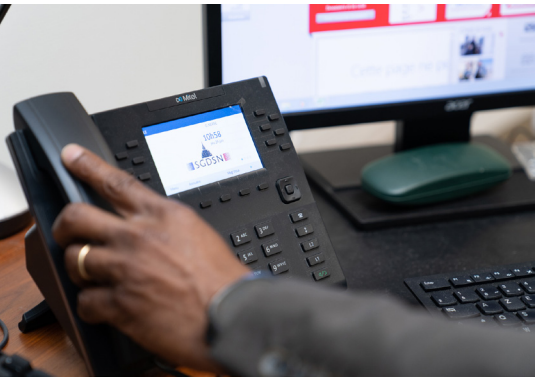
L'enjeu principal est celui du changement d'échelle. Comme l'a montré notre *Panorama de la cybermenace*, nous sommes confrontés à une menace croissante et toujours mieux organisée. Tant les acteurs étatiques que les groupes cybercriminels continuent d'accentuer leur action et perfectionnent leurs modes opératoires. Cette pression qui ne se dément pas met l'ANSSI et l'ensemble de l'écosystème au défi de s'adapter.

En 2023 et 2024, la France sera l'hôte de deux grands événements internationaux : la Coupe du monde de rugby et les jeux Olympiques et Paralympiques. Les défis en matière de cybersécurité seront donc encore accentués. Nous travaillons déjà à anticiper ces événements, qui imposent à l'agence et à ses partenaires de donner le meilleur d'eux-mêmes.

En outre, la transposition de la directive *NIS2* devrait considérablement accroître le périmètre d'intervention de l'agence en élargissant le nombre d'opérateurs assujettis à des diligences particulières en matière de cybersécurité. Cette extension va nécessiter une révision de nos méthodes de travail et une refonte de la relation que nous entretenons avec les opérateurs relevant de notre périmètre de responsabilité.

Ces défis mobilisent l'ensemble des agents de l'ANSSI et font l'objet d'un dialogue constant avec nos autorités et nos partenaires. ◄

ACCÉLÉRER LA SÉCURISATION NUMÉRIQUE DE L'ÉTAT



Après une année consacrée à la mise en place de l'organisation de l'opérateur des systèmes d'information interministériels classifiés (OSIIC), l'année 2022 a été marquée par sa montée en puissance : accueil et intégration de nouveaux arrivants aux profils variés ; développement d'une identité propre ; maîtrise des fonctions de soutien ; élaboration d'une feuille de route pour les prochaines années et insertion dans l'écosystème des nouveaux bénéficiaires.

Préparer la gestion de crise tout en assurant l'urgence opérationnelle

Au service de l'État et du SGDSN, l'OSIIC a concouru activement à l'action collective dans le domaine de la stratégie nationale de résilience (SNR), de la gestion de crise et dans la préparation des rendez-vous majeurs de 2023 et 2024. L'opérateur a modernisé les moyens de communication des très hautes autorités de l'État et s'est restructuré pour répondre plus efficacement aux besoins opérationnels des ministères.

ANTICIPATION ET MAILLAGE TERRITORIAL

Dans le domaine de l'interministériel, l'effort de déploiement s'est poursuivi. Les échanges avec les ministères ont été repensés et la gouvernance totalement rénovée, afin de gagner en efficacité. Les résultats sont au rendez-vous, avec notamment la fin de la mise en place de la nouvelle architecture réseau et un doublement du nombre des terminaux classifiés déployés. Fin 2022, plus de 4 400 terminaux équipaient plus de 600 sites, assurant ainsi une couverture complète du territoire métropolitain et ultramarin. Ce maillage permet de préparer les futures échéances majeures que sont la Coupe du monde de rugby et les jeux Olympiques et Paralympiques de Paris en 2024. Au-delà, ils permettront de faciliter la conduite et la gestion de crise par les services de l'État. Par ailleurs, le projet des *hubs* interministériels, entré dans sa phase pilote, permettra à l'ensemble des services de l'État d'accéder à des moyens de communication classifiés sur tout le territoire.

MODERNISATION DES MOYENS DE COMMUNICATION DES TRÈS HAUTES AUTORITÉS

Le projet COMGOUV-NG, nouveau service de télécommunications sécurisées mis en place dans l'avion à usage gouvernemental et le déménagement des moyens techniques à l'Élysée ont permis à l'OSIIC de réaliser les premières étapes d'une évolution plus générale des moyens de communication classifiés des très hautes autorités de l'État. Lorsqu'il se déplace à l'étranger, le Président de la République doit pouvoir disposer d'une capacité de communication équivalente à celle qu'il emploie sur le territoire national. La solution de téléphonie classifiée a donc été généralisée en remplacement du système de téléphonie existant devenu obsolète et complétée par la mise en service de moyens de communication classifiée projetables lors des voyages officiels, en remplacement des points mobiles de communication « historiques ».

RÉPONDRE À L'URGENCE OPÉRATIONNELLE

Désormais, l'OSIIC s'appuie sur le centre de mise œuvre – CMO – pour la conduite des opérations et la supervision des moyens de communication interministériels. Ce dispositif est complété par l'assistance numérique, joignable en permanence par les agents du SGDSN et ceux des ministères ou des services déconcentrés. Cette restructuration, rendue indispensable par la complexité et l'étendue des systèmes déployés, démontre quotidiennement sa pertinence et répond aux attentes des utilisateurs.

Accompagner la transformation numérique du SGDSN

L'année 2022 aura aussi été marquée par la profonde transformation de l'environnement numérique du SGDSN, notamment en matière de mobilité, et par les nouvelles pratiques de travail nées de la crise sanitaire.

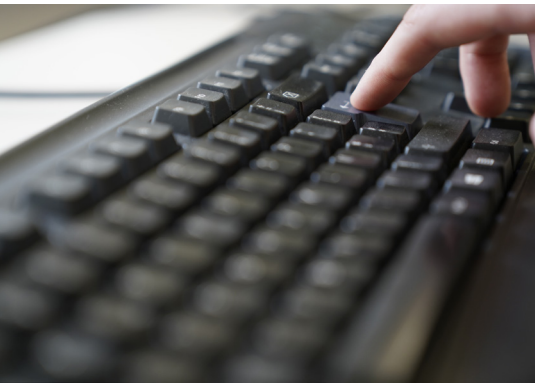
UNE OFFRE NUMÉRIQUE RÉNOVÉE

En un temps record et dans le prolongement de la crise sanitaire, l'OSIIC a adapté son offre numérique en généralisant sur l'environnement de travail numérique des agents du SGDSN le portefeuille de ses applications. L'offre des services en mobilité a été étendue à tous les agents du SGDSN et étoffée d'outils interministériels, comme les services d'audioconférence et de visioconférence protégés, qui permettent aujourd'hui au SGDSN de bénéficier d'outils internes sécurisés, adaptés aux besoins de communication en mobilité.

Par ailleurs, la contribution de l'OSIIC au projet de mobilité sécurisée NEO2 du ministère de l'intérieur et des outre-mer, fondé sur la solution Secdroid, lui a permis de consolider son expertise dans le domaine de la mobilité sécurisée et de franchir ainsi un jalon important dans l'évolution des terminaux mobiles sécurisés déployés auprès des agents du SGDSN. En effet, la conception, le développement, le soutien et les évolutions du « socle système » sont portés par l'OSIIC.

À L'ÉCOUTE DE LA COMMUNAUTÉ DES RÉFÉRENTS NUMÉRIQUES

Pour accompagner au mieux la transformation numérique du SGDSN, prendre en compte les demandes « métier » et intégrer les attentes des utilisateurs, l'animation de la communauté des référents numériques des directions et services du SGDSN a démontré toute son utilité. Interlocuteur privilégié de l'opérateur, le référent est le garant de la cohérence entre les enjeux, les besoins et les priorités numériques de son unité organisationnelle et la stratégie numérique globale de l'OSIIC. ▶▶▶



Adapter nos systèmes aux exigences de demain

L'année 2022 fut une année de mise à niveau des infrastructures, d'études, de réflexions et de conduite de nombreux travaux de groupe, notamment en vue de la refonte des systèmes d'information interministériels classifiés. Ces travaux conditionneront les développements menés par l'OSIIC dans les années à venir.

DÉCOMMISSIONNEMENT ET RATIONALISATION DES INFRASTRUCTURES

L'OSIIC a fourni un gros effort de rationalisation et de retrait de terminaux obsolètes, mais aussi d'applications désuètes ou inutilisées, comblant ainsi une partie de sa dette technique. L'extinction du réseau RIMBAUD (Réseau interministériel de base uniformément durci), la désaffection de ses infrastructures, la réintégration d'une grande partie de la flotte des anciens téléphones mobiles classifiés ainsi que le démantèlement de réseaux téléphoniques obsolètes auront marqué l'année 2022.

L'effort a également porté sur la fermeture d'infrastructures d'hébergement anciennes et la mise en place d'un hébergement à l'état de l'art d'un nouveau *data center*. Ces réalisations préparent les futurs chantiers et notamment celui de rationalisation de l'ensemble des réseaux de l'OSIIC.

REFONTE DES SYSTÈMES D'INFORMATIONS INTERMINISTÉRIELS CLASSIFIÉS

La mise à niveau de l'infrastructure s'est déclinée en plusieurs chantiers. La nouvelle architecture réseau est désormais déployée sur 500 sites. Plus de 2 000 nouveaux postes bureautiques de niveau classifié ont ainsi été installés, en parallèle des nouveaux déploiements. L'OSIIC a également consulté référents et utilisateurs, tant des ministères que du SGDSN, pour préparer un chantier structurant et prioritaire destiné à faire converger les moyens de communication classifiés (téléphonie, visioconférence, bureautique…).

Une première étape de ce projet est désormais engagée. Elle initie la convergence des moyens bureautiques et des moyens téléphoniques de communication et le développement de nouvelles capacités et services collaboratifs pour l'ensemble des ministères, mais aussi de services spécifiques au SGDSN, permettant de remplacer progressivement le réseau interne classifié du SGDSN. La convergence des systèmes et des infrastructures permettra de rationaliser les développements futurs et de simplifier l'exploitation des systèmes d'information et de communication. Cette démarche offrira ainsi davantage de fonctionnalités aux utilisateurs de ces systèmes, en interministériel comme au sein du SGDSN, tout en renforçant leur fiabilité et leur sécurité. ◄

Questions à...

Colonel Pascal Florin

Directeur adjoint
des systèmes d'information
interministériels classifiés
(OSIIC)

Par décret du Président de la République, Yves Verhoeven a été nommé directeur de l'Opérateur des systèmes d'information interministériels classifiés (OSIIC) le 7 juin 2023.

Comment l'OSIIC fait-il face à la demande croissante de moyens classifiés en interministériel ?

Afin de répondre aux besoins croissants en systèmes d'information interministériels classifiés, d'optimiser l'organisation des déploiements et de s'assurer de la satisfaction des bénéficiaires, l'OSIIC a élaboré depuis sa création un schéma directeur des déploiements des systèmes d'information interministériels classifiés. Ce schéma directeur a permis de recenser les besoins, de prioriser, puis de cadencer les déploiements. Il est mis à jour régulièrement avec nos partenaires des ministères et validé au sein d'instances de gouvernance interministérielles.

Pour répondre de façon plus efficace à la demande, l'OSIIC a initié un projet de *hubs* interministériels. Ce projet revêt une grande importance pour l'opérateur et plus généralement pour le SGDSN. D'une part, il permettra à l'ensemble des services de l'État d'accéder à des moyens de communication classifiés sur l'ensemble du territoire, notamment pour remplacer le réseau RIMBAUD et pallier le retrait des terminaux

TEOREM-RIMBAUD ; d'autre part, il optimisera les déploiements dans un souci d'efficience. Ce projet favorise ainsi la rationalisation des moyens et répond notamment aux besoins épisodiques ou ponctuels de nombreux organismes d'accéder à de tels moyens, sans que cela justifie les investissements nécessaires à la mise en place de ces moyens dans leurs propres locaux. Ainsi les agents de ces organismes, habilités au secret de la défense nationale et de nationalité française, ayant un besoin ponctuel de consulter ou d'échanger des informations classifiées peuvent se rendre sur le site où le *hub* a été ouvert afin d'accéder à ces moyens mutualisés.

Dans un premier temps, grâce à l'investissement personnel du préfet Didier Martin, secrétaire général et haut fonctionnaire de défense et de sécurité nationale du ministère de l'intérieur, deux sites pilotes ont été proposés par le ministère de l'intérieur et des outre-mer : Fort-de-France et Lille. Pour sa part, le ministère des armées a proposé les sites de Marseille et Metz.

Dans un second temps, ces *hubs* interministériels sont entrés dans la phase « pilote », avec l'ouverture le 1er septembre 2022 du premier d'entre eux situé à Fort-de-France, puis du deuxième, à Marseille au mois de mars 2023.

Après l'ouverture des quatre sites pilotes, une généralisation du dispositif a été envisagée à partir de mi-2023.

Où en est le grand projet *Datacenter* ?

En 2015, le projet *Datacenter* a été initié pour répondre à l'évolution nécessaire des systèmes d'information ainsi qu'aux besoins des entités du SGDSN.

Ce projet avait un double objectif : la modernisation des systèmes d'information et de leur hébergement, d'une part, et l'extension de leurs capacités, d'autre part.

Ce projet a pu voir le jour grâce à un partenariat avec le ministère de l'intérieur et des outre-mer. Le bâtiment, qui a été livré 1er novembre 2018, est localisé dans une emprise de la gendarmerie nationale en Île-de-France. Cette emprise est hautement sécurisée et présente des garanties élevées en matière de résilience.

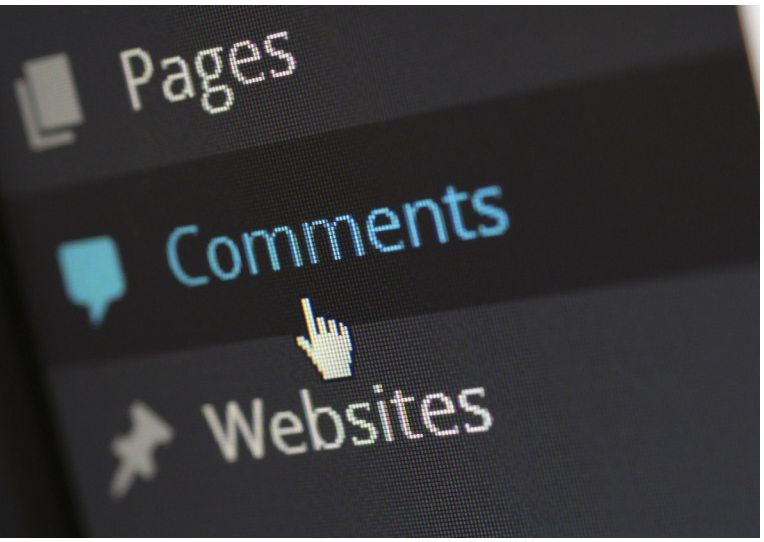
Le *Datacenter* est entré officiellement en production au printemps 2019, avec l'installation des premiers équipements. Il est devenu un élément central dans la nécessaire refonte du socle technique exploité par l'OSIIC. Certaines entités du SGDSN y hébergent déjà une partie de leurs systèmes d'information.

Pour aller au-delà, de nouvelles technologies, comme la virtualisation et l'automatisation de nos outils de production, doivent également nous aider à faire évoluer nos systèmes d'information. Bref, le *Datacenter* nous apporte de la fiabilité et une amélioration dans nos processus de travail.

Il s'agit là de concrétiser l'un des axes majeurs du schéma directeur de l'OSIIC, à savoir la rationalisation de notre système d'information, qui est aujourd'hui vieillissant. ◂

CONTRER LES MANIPULATIONS DE L'INFORMATION

CONTRER LES MANIPULATIONS DE L'INFORMATION



Crée à l'été 2021, Viginum est le service technique et opérationnel de l'État chargé de protéger le débat public contre les campagnes numériques de manipulation de l'information. Il a pour missions principales de détecter et de caractériser les ingérences numériques étrangères répondant aux quatre critères suivants :

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

Pour ce faire, les agents de Viginum explorent les contenus publiquement accessibles en ligne, sur les plateformes, sites et médias numériques afin de mettre en évidence les phénomènes qui remplissent ces critères.

Les missions et les activités de Viginum s'insèrent dans un cadre juridique strict, reposant principalement sur deux décrets : le décret n° 2021-922 du 13 juillet 2021 portant création du service ainsi que le décret n° 2021-1587 du 7 décembre 2021 autorisant le service à mettre en œuvre un traitement automatisé de données à caractère personnel. Au cours de sa première année d'existence, le service a pris, en lien avec les services de la CNIL, plusieurs décisions importantes afin de se conformer à ses obligations réglementaires, parmi lesquelles la désignation d'une référente « informatiques et libertés ».

L'activité de Viginum fait, par ailleurs, l'objet d'un suivi rigoureux de la part du comité éthique et scientifique, placé auprès du secrétaire général de la défense et de la sécurité nationale. Viginum met à disposition du comité tous les documents et informations utiles à l'accomplissement de sa mission, notamment les notes d'analyse qu'il produit. Le comité éthique et scientifique peut adresser au chef de service des questions, des observations ou des recommandations. Il a publié en 2023 son premier rapport public remis à la Première ministre.◀

Une première année d'opérations

Lors de sa première année d'existence, Viginum a consacré la majeure partie de son activité à la protection des grands rendez-vous électoraux de l'année 2022, moments particulièrement propices aux ingérences numériques étrangères.

Viginum s'est également mobilisé pour identifier les comportements inauthentiques pouvant affecter le débat public numérique en réaction aux grands événements qui ont marqué l'actualité nationale ou internationale, telle que la guerre en Ukraine. Durant l'année 2022, hors opérations électorales, Viginum a détecté plus de 78 phénomènes potentiellement inauthentiques, susceptibles de révéler une ingérence numérique étrangère. Sept ingérences ont été caractérisées.

Un collectif de travail et une équipe pluridisciplinaire

L'un des enjeux majeurs de la première année d'existence de Viginum a été de recruter et de structurer son collectif de travail. Par une politique de communication et de recrutement ciblée, Viginum s'est attaché à rassembler différents métiers et savoir-faire indispensables à la bonne réalisation de ses missions et à faire émerger un collectif de travail adapté à la nature protéiforme de la menace informationnelle. Aujourd'hui, le service s'appuie sur une équipe pluridisciplinaire : spécialistes en investigation et analyse numériques (OSINT), professionnels d'Internet et du marketing numérique, experts en science de la donnée, ingénieurs en systèmes d'information, spécialistes en sciences politique et géopolitique. ▶▶▶

La sécurisation des élections

Du 9 novembre 2021 au 20 juillet 2022, les équipes de Viginum ont successivement ouvert et suivi deux opérations visant à la sécurisation de l'élection présidentielle d'avril 2022 et du scrutin législatif du mois de juin 2022 dans les champs informationnel et numérique.

Durant ces opérations, les équipes ont apporté une attention particulière aux narratifs susceptibles de porter atteinte aux candidatures, au bon déroulement du débat (quels qu'en soient les thèmes) ainsi qu'à la crédibilité de la procédure électorale (avant et après le scrutin). À cette occasion, Viginum a affermi ses liens avec d'autres administrations qui participent, directement ou indirectement, à la lutte contre les manipulations de l'information. Durant cette période, le service a également entretenu un dialogue étroit avec les autorités garantes du bon déroulement de l'élection présidentielle (Conseil constitutionnel, Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle, Autorité de régulation de la communication audiovisuelle et numérique). Au bilan, Viginum a détecté plus de 60 phénomènes inauthentiques sur les plateformes numériques, dont 12 ont fait l'objet d'investigations approfondies à des fins de caractérisation et 5 ont été positivement caractérisées comme des ingérences numériques étrangères. ◀

Nombre de personnes recrutées au cours de l'année 2022

27
recrutements (hors stages)
avec un total de

50
personnes au sein du service

En 2022, pendant la période électorale :

60
phénomènes potentiellement inauthentiques détectés

5
opérations d'ingérence numérique étrangères caractérisées

En 2022, hors questions électorales :

78
phénomènes potentiellement inauthentiques détectés

7
opérations d'ingérence numérique étrangères caractérisées

Le premier rapport public de Viginum a été publié le 25 octobre 2022. Il est disponible sur le site du SGDSN.

Un écosystème mobilisé pour lutter contre les manipulations de l'information

L'action de Viginum s'inscrit dans un écosystème national et international contribuant à la lutte contre les manipulations de l'information.

À ce titre, Viginum a mis à profit sa première année d'existence pour consolider le réseau composé des administrations dotées de capacités opérationnelles en matière de lutte contre les manipulations de l'information. Les efforts engagés pour animer au quotidien ce réseau ont permis d'assurer des échanges fluides et réactifs de nature technique, opérationnel et méthodologique pour faire face aux manipulations de l'information et ingérences numériques étrangères.

Viginum a également activement assisté le secrétaire général de la défense et de la sécurité nationale dans ses missions et travaux de coordination interministériels en matière de lutte contre les manipulations de l'information, notamment au sein du comité de lutte contre les manipulations de l'information (COLMI).

En complément, Viginum a échangé avec des partenaires étrangers parmi les plus exposés à la menace informationnelle. En 2022, le service a également noué de premiers contacts avec des acteurs clés de la sphère académique qu'il approfondira tout au long des années à venir. ◄

Questions à...

Gabriel Ferriol

Chef du service de vigilance et de protection contre les ingérences numériques étrangères, (Viginum)

Presque deux ans après sa naissance, comment se porte Viginum ?

Viginum se porte bien. Après une période de mise en place et d'expérimentation dans la deuxième moitié de l'année 2021, suivie d'une intense séquence d'engagement opérationnel au printemps 2022 pour la protection des scrutins nationaux dans le champ informationnel, nous sommes désormais entrés dans une phase de consolidation et de maturation.

Au plan opérationnel, cette phase s'est traduite, d'une part, par une réorganisation de notre portefeuille d'opérations, que nous avons rationalisé en lien avec le secrétaire général, pour l'adapter au mieux à l'évolution des menaces, et d'autre part, par une simplification de nos procédures opérationnelles, pour accroître notre agilité et notre réactivité tout en développant notre force de frappe. Ces évolutions ont permis à Viginum d'aguerrir ses capacités d'analyse technique, d'élargir le spectre des menaces appréhendées et de mettre au jour de nombreux phénomènes d'intérêt.

Dans le même esprit, Viginum s'est fixé, à l'automne 2022, l'objectif de

consolider ses liens avec la sphère académique. Un colloque s'est tenu au mois de juin 2023, destiné à favoriser les interactions entre les acteurs de l'écosystème.

Nous continuons par ailleurs de grandir et progresser dans de multiples dimensions (formation, méthodologie, outils, systèmes d'information, gestion des ressources humaines, coopération internationale, etc.).

Comment Viginum participe-t-il à la lutte contre les ingérences numériques étrangères ?

Tout au long de l'année 2022, Viginum s'est attaché à structurer et à animer les travaux interministériels menés dans le cadre du COLMI-TECH qui rassemble l'ensemble des administrations dotées de capacités opérationnelles en matière de lutte contre les manipulations de l'information. À ce titre, Viginum a joué un double rôle : en tant qu'animateur, le service a organisé plusieurs cycles de réunions, rencontres, ateliers thématiques ou méthodologiques ; en tant que contributeur, Viginum a adressé aux autres membres du réseau de nombreux relevés de détection rendant compte de phénomènes inauthentiques susceptibles de révéler l'existence d'ingérences numériques étrangères.

Depuis le début de l'année 2023, Viginum assume en outre désormais un rôle plus important dans l'organisation et dans le fonctionnement du comité opérationnel de lutte contre les manipulations de l'information (COLMI). Par sa connaissance de la menace et son expertise technique, Viginum entend ainsi contribuer le plus possible non seulement à la détection et à la caractérisation des manœuvres informationnelles hostiles émanant de nos compétiteurs stratégiques mais également à la protection contre ces manœuvres, en lien avec l'ensemble des départements ministériels compétents (affaires étrangères, armées, intérieur, etc.).

Quels sont désormais les principaux enjeux à venir pour Viginum ?

L'aventure ne fait que commencer. Tout au long de l'année 2023, Viginum va continuer de consolider ses procédures opérationnelles, en portant une attention particulière à leur confidentialité vis-à-vis de nos compétiteurs stratégiques ainsi qu'à leur conformité juridique et éthique. Nous ambitionnons également de franchir en 2023 plusieurs paliers importants au plan capacitaire, au travers de la mise au point et de l'industrialisation d'une palette d'outils souverains. Ces outils doivent permettre à Viginum de disposer d'une appréciation autonome de la menace informationnelle mais également de faire émerger un maximum de synergies entre les différentes compétences (investigation en sources ouvertes, géopolitique, *data science*, *digital marketing*…) rassemblées dans son collectif de travail.

Enfin, ces derniers mois, Viginum a noué de nombreux contacts avec des partenaires internationaux, préoccupés ou même directement exposés à la menace informationnelle. Ces échanges bilatéraux ou multilatéraux ont permis de comparer les approches opérationnelles des uns et des autres, de recueillir et de partager des bonnes pratiques ainsi que de faire émerger une appréciation commune de certaines menaces. Ces premiers contacts, initiés pour la plupart en 2022, laissent augurer une année 2023 résolument placée sous le signe de la coopération internationale en matière de lutte contre les manipulations de l'information. ◂

SOUTENIR LE RENSEIGNEMENT

Le GIC emploie des développeurs, des administrateurs réseau et système, des chefs de projets informatiques et de nombreux autres spécialistes déterminés à exercer des métiers opérationnels exigeants et sensibles.

Le SGDSN soutient l'activité du groupement interministériel de contrôle et accompagne sa croissance.

Depuis 2015, le flux annuel de demandes de techniques de renseignement traité par le GIC a considérablement augmenté. Cette hausse ne s'est pas démentie en 2022. Pour autant, la tendance est à un ralentissement du rythme de croissance, laissant entrevoir une forme de stabilisation à terme.
La hausse par rapport à 2021 est contrastée : lors des périodes de confinement sanitaire, les techniques de proximité ont été moins utilisées que celles de recueil à distance. Cette situation s'est inversée une fois ces périodes de confinement achevées.

Connaissant une croissance ininterrompue depuis 2016, les techniques de recueil à distance marquent le pas. Les géolocalisations en temps réel n'ont progressé que de 10 % alors que les taux d'accroissement annuels étaient de l'ordre de 30 % à 40 % depuis 2016. Le nombre d'interceptions de sécurité s'est stabilisé. Les identifications connaissent un léger recul et le nombre d'autorisations de surveillance internationale a baissé.

En 2022, le GIC a consacré une part importante de son activité à faire évoluer ses prestations. Il a adapté ses locaux pour améliorer les conditions d'accueil des exploitants : cinq centres d'exploitation ont été rénovés ou déplacés, dont trois outre-mer. Il a formé 487 agents des services à l'utilisation de ses logiciels. Il a simplifié les procédures dématérialisées permettant d'assurer la traçabilité des techniques de renseignement. Il a mené à bien plusieurs évolutions majeures des outils informatiques qu'il met à disposition des exploitants. Il a installé plusieurs centaines de postes de travail sur ses 82 sites informatiques.

Unique détenteur du pouvoir de réquisition des opérateurs de communications électroniques, des fournisseurs d'accès à Internet et des hébergeurs de sites pour la mise en œuvre des techniques de renseignement, le GIC a établi des liens sécurisés avec de nouveaux acteurs du numérique pour être en mesure de recueillir plus de données stockées ou en transit, à la demande des services.

Le GIC a lancé un programme de fiabilisation de ses infrastructures informatiques et de rationalisation de ses architectures, après six années marquées par le déploiement de multiples systèmes d'information distincts, destinés à satisfaire aux exigences opérationnelles ou rendus nécessaires par les fréquentes évolutions du cadre légal entre 2016 et 2021. Ces travaux sont indispensables pour assurer la permanence des missions du GIC, avec un niveau de fiabilité à la hauteur des enjeux de sécurité nationale auxquels elles contribuent.

En 2022, le GIC a consenti un effort particulier pour la sécurité de ses systèmes d'information en consolidant son centre de détection et en parvenant à réduire drastiquement le nombre de fausses alertes, grâce à un ensemble sophistiqué d'algorithmes. Ces avancées ont été complétées par l'installation de nouveaux outils de détection comportementale et d'analyse de vulnérabilités sur les postes de travail.

La loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement a confirmé la position centrale du GIC au cœur du dispositif des techniques de renseignement :

- le GIC est conforté par la loi comme le seul organisme autorisé à mettre en œuvre les algorithmes destinés à prévenir les actes de terrorisme. Ces algorithmes, expérimentaux jusqu'alors, sont pérennisés. L'équipe de programme du GIC peut donc engager des développements plus ambitieux ;
- en encadrant les transmissions de renseignement entre les services, la loi a confié au GIC le soin de centraliser les demandes et les relevés de transmission ;
- pour rendre possible l'interception des communications par satellite lorsque l'opérateur ne défère pas à ses obligations, la loi a également prévu un régime centralisé au GIC pour que de telles interceptions soient possibles et soient traitées avec les mêmes garanties que les interceptions de sécurité ;
- enfin, la loi a étendu le pouvoir de réquisition du GIC auprès des opérateurs de communications électroniques, des fournisseurs d'accès à Internet et des hébergeurs de sites pour faciliter la mise en œuvre de certaines techniques de renseignement.

Chacune de ces dispositions a donné lieu en 2022 à des travaux soutenus de la part des agents du groupement.

Pour la première fois de son histoire, le GIC a accueilli une réunion internationale portant sur la standardisation des interceptions légales, à laquelle ont été associés les partenaires institutionnels du groupement : l'agence nationale des techniques d'enquêtes numériques judiciaires et le commissariat aux communications électroniques de défense. Des contacts ont pu être établis avec certains homologues étrangers en vue de futures discussions bilatérales, à des fins de comparaison des cadres juridiques et des méthodes de recueil.

Avec le soutien du SGDSN, le GIC a gréé en 2022 tous les emplois ouverts et a légèrement surconsommé sa dotation budgétaire. L'accroissement des effectifs, dans l'attente d'une installation début 2024 dans un nouveau bâtiment situé en proche banlieue qui com-

Chiffres clés

360
autorisations de techniques de renseignement par jour

487
formations dispensées aux agents des services pour l'utilisation des applications du GIC

Des systèmes d'information sécurisés

82
sites

6 000
utilisateurs

plétera le site parisien principal, a nécessité une nouvelle recherche, fructueuse, de locaux provisoires dans lesquels une partie des équipes techniques du GIC se sont installées.

Dans une structure comptant 250 agents répartis sur plusieurs sites, accueillant des milliers d'exploitants des services, permanents ou vacataires, il est apparu nécessaire de consacrer un effort particulier à la prévention, à la sécurité et au bien-être au travail. Le groupement s'est organisé à cette fin, en procédant à des recrutements spécifiques. En parallèle, grâce à l'allègement des contraintes sanitaires, dans un contexte où de nouvelles pratiques se sont installées (fonctionnement multi-sites, télétravail), des actions de communication interne et de cohésion ont été menées, facilitant la mobilité interne et la fluidité des rapports professionnels.

L'année 2023 est pour le GIC celle de deux enjeux importants : d'une part, donner leur pleine efficacité aux algorithmes pour la prévention du terrorisme, méthode de détection prometteuse dans un contexte où la menace est forte mais ses signaux sont faibles ; d'autre part, mener à bien les travaux d'aménagement d'un bâtiment supplémentaire pour le GIC, qui accueillera des exploitants parisiens dans des locaux adaptés en 2024 et augmentera significativement les capacités de stockage et de calcul du GIC.

En 2023, le GIC devra toujours son efficacité au talent de ses agents, pleinement engagés au service de la sécurité nationale, dans le respect des valeurs de la République et de la vie privée de nos concitoyens. ◂

Centralisation des techniques de renseignement

UN SERVICE DE L'ADMINISTRATION GÉNÉRALE PERFORMANT ET PROCHE DE TOUS

Le service de l'administration générale (SAG), service à vocation transversale du SGDSN, anime et coordonne l'ensemble des missions d'administration générale nécessaires à l'activité du secrétariat général et des services à compétence nationale qui lui sont rattachés, ainsi qu'à celle du groupement interministériel de contrôle.

Le service, qui est organisé en deux sous-directions (ressources humaines ; administration générale et finances) et un détachement de gendarmerie, emploie une centaine d'agents de statuts divers.

Ressources humaines

SOUTENIR DES EFFECTIFS EN HAUSSE…

L'augmentation des effectifs du SGDSN s'est poursuivie en 2022, avec une progression de 101 emplois en 2022, contre 62 en 2021. L'année 2022 aura aussi été celle de la mise en place d'une gestion des ressources humaines rénovée pour aider à la réalisation des missions interministérielles du SGDSN.

POLITIQUE SALARIALE

En 2022, le SGDSN a renforcé sa politique d'attractivité et de fidélisation des compétences. Une adaptation des grilles salariales des métiers du numérique, développée de concert avec l'ANSSI, a permis de maintenir les propositions salariales du SGDSN à un niveau élevé parmi celles de l'ensemble des services de l'État.

DÉVELOPPEMENT D'UNE IDENTITÉ ET D'UNE CULTURE COMMUNE

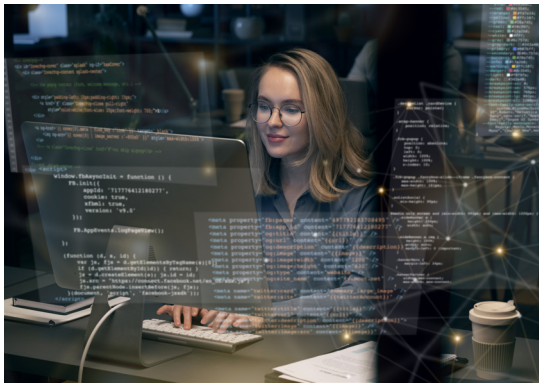
Dans le cadre de la nouvelle politique du Gouvernement en matière d'attractivité et la valorisation de la marque employeur des services publics, la « place emploi public »[1] et la participation aux salons de l'emploi constituent des vecteurs du déploiement de la marque employeur des services publics. Dans ce cadre, le SGDSN a procédé à une refonte de sa page internet « Espace recruteurs » afin de valoriser auprès des candidats les valeurs qui constituent son identité.

RENFORCEMENT DE L'ACCOMPAGNEMENT DES AGENTS

- **Un budget « formation »** : En consacrant en 2022, plus d'1 million d'euros à la formation de ses agents, le SGDSN investit dans l'avenir en souhaitant développer les compétences de ses personnels.
- **La valorisation de la mobilité interne** : Les principes de la mobilité interne du SGDSN s'inscrivent dans le cadre des lignes directrices de gestion des services de la Première ministre du 24 janvier 2020 et ont été diffusés à l'ensemble des agents du SGDSN. En 2022, les différentes procédures d'accompagnement dont peuvent bénéficier les agents ont fait l'objet de diverses communications permettant de mieux identifier les outils proposés par la conseillère en évolution professionnelle : point carrière, bilan de compétence, préparations aux concours…

1. Devenu « choisir le service public » en 2023

- **L'optimisation du processus d'intégration des agents** : Le SAG, en collaboration avec les directions, a souhaité passer en revue l'ensemble du processus d'intégration des agents. Une refonte a permis d'avancer dans trois domaines : une meilleure transmission des informations entre les interlocuteurs ; une meilleure préparation en amont de l'arrivée d'un nouveau collègue ; un accueil mieux maîtrisé le jour « J ». Ces trois préalables, désormais remplis, sont nécessaires à la mise en place prochaine d'une expérimentation de mentorat.
- **La participation à des forums** : En 2022, les personnels SGDSN ont été invités à participer à différents séminaires, notamment le programme « Talents féminins du numérique », organisé par la DINUM, qui proposait aux femmes travaillant dans les métiers du numérique au sein de l'État un accompagnement dans l'évolution de leur carrière.



UNE TRANSFORMATION RH « EFFECTIVE »

Les équipes de la sous-direction « ressources humaines » ont été fortement mobilisées afin de mettre à disposition des *managers* et des agents plusieurs outils pratiques : guide du recrutement, passeport formation à l'ANSSI, tout en veillant à la promotion de l'inclusion de tous. Dans ce cadre, l'année 2022 aura été marquée par la première participation du SGDSN au Duo Day et la signature d'une convention de mécénat en faveur de la réinsertion par le sport des militaires blessés.

L'AMÉLIORATION DU CADRE DE TRAVAIL

L'amélioration du cadre de travail constitue un fort enjeu. À cet effet, différentes actions ont été conduites permettant au personnel d'évoluer dans un environnement de travail bienveillant et éco-responsable. Outre les initiatives du SGDSN (*footing*, événements de cohésion divers…), le SAG a relayé différentes initiatives de la DSAF, notamment la participation des personnels du SGDSN au forum sur la qualité de travail.

L'effort consenti depuis plusieurs années pour la promotion de la santé et du bien-être des agents a été maintenu en 2022, au travers de plusieurs projets.

Ainsi, le réseau de prévention a organisé diverses activités : séances d'information lors des réunions d'accueil des nouveaux arrivants ; campagne de communication sur la prévention permettant la mise en avant de nombreux thèmes, allant de la prévention des risques psychosociaux à l'ergonomie du poste de travail, en passant par la promotion de l'activité physique, entre autres.

UN DIALOGUE SOCIAL « RÉNOVÉ »

Enfin, l'année 2022 aura été marquée par un événement majeur de la vie professionnelle des agents : la tenue des élections professionnelles dans le cadre de la réforme des instances de dialogue social et le renforcement de la négociation collective qui a généralisé le système de vote électronique et mis en place les nouvelles instances de dialogue social. Il est important de souligner que l'institution du comité social d'administration contient, en son sein, une formation spécialisée en matière de santé, de sécurité et des conditions de travail, laquelle disposera de prérogatives jusqu'alors dévolues aux CHSCT. En utilisant, les différents outils mis à sa disposition (lignes directrices de gestion, rapport social unique), le SGDSN aura pour mission d'instaurer avec les représentants nouvellement élus, un dialogue constant. ▶▶▶

Administration générale et finances

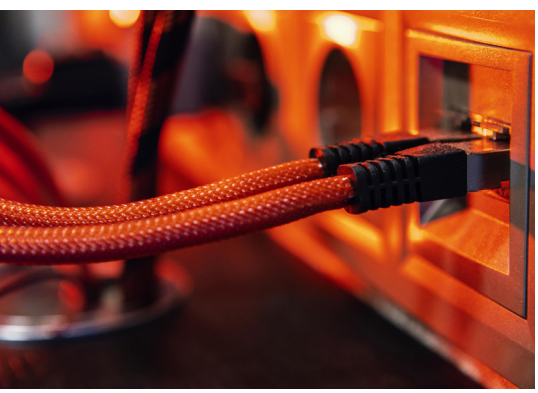
En 2022, l'organisation de la sous-direction a significativement évolué. Son périmètre de responsabilité a été élargi avec le rattachement de la division « immobilier et soutien aux services ». Il en a résulté un doublement du nombre des agents employés dans l'ensemble de la sous-direction.

L'activité du domaine achats-finances est demeurée soutenue avec un budget total administré, toutes ressources comprises, de 215,3 M€ en autorisations d'engagement et 219,3 M€ en crédits de paiement. L'année 2022 aura été plus particulièrement marquée par :

- la montée en puissance du service à compétence nationale Viginum, en lien avec le développement de ses capacités et l'atteinte de sa cible en emplois ;
- la poursuite d'opérations d'infrastructures ou immobilières d'ampleur, notamment la construction et l'aménagement de nouvelles emprises pour l'ANSSI, l'OSIIC et le GIC ;
- le maintien d'une politique dynamique de développement et d'acquisition d'équipements et logiciels informatiques dans le cadre de la conduite de la politique de sécurité des systèmes d'information et du renforcement des communications électroniques sécurisées de l'État ;
- le soutien au financement de programmes interministériels contribuant à la caractérisation et à la lutte contre certaines menaces ou au développement de capacités techniques, au titre de la coordination en matière de défense et de sécurité.

Parallèlement, la mise en œuvre du volet « sécurisation des systèmes numériques de l'État et des territoires » du plan d'investissement France Relance s'est poursuivie. L'enveloppe budgétaire initiale de 136 M€ a fait l'objet d'un abondement complémentaire de 40 M€, en 2022. Au total, ce sont donc 176 M€ qui auront été engagés dans cette action en 2021 et 2022. Les années 2023 et 2024 seront consacrées à la finalisation du paiement des actions engagées dans ce cadre.

En termes purement quantitatifs, l'activité financière s'est ainsi traduite par 4 409 demandes de paiements. 1069 subventions ont été traitées au seul titre du plan France Relance et 82 engagements dans le cadre des arrivées des apprentis et des stagiaires. Concernant les déplacements et les missions, 4 489 ordres de mission auront été traités.



En parallèle, la notification de 53 nouveaux marchés ainsi que l'établissement de 2 470 bons de commande quantifient le niveau d'activité du bureau achats-marchés durant cette année, pour accompagner les services du SGDSN sur un large spectre de besoins. Le bureau achats-marchés a également été fortement mis à contribution par la direction des achats de l'État pour l'élaboration de son plan des achats. Il a en outre participé activement à la mise en place du comité ministériel de suivi des prestations intellectuelles.

Sur le volet immobilier et soutien général, l'année 2022 a également été particulièrement active que ce soit pour :

- le bureau **infrastructure**, qui a poursuivi ses actions d'entretien, de maintenance et de travaux sur les différents sites occupés par le SGDSN, tout

en répondant aux contraintes liées notamment à la mise en sécurité des installations techniques.
Les forts enjeux relatifs à l'augmentation des effectifs ont été l'occasion en 2022 de lancer un audit d'occupation pour analyser les possibilités d'optimisation des espaces de bureaux.
L'année 2022 a également vu le lancement de l'opération de transformation d'un bâtiment localisé au Mont-Valérien pour le substituer au site d'entreposage de Pantin. Par ailleurs, des études d'aménagement d'un bâtiment historique au sein de l'Hôtel national des Invalides ont été lancées, afin d'y aménager des espaces de travail ;

- la **logistique**, qui a mené 182 opérations de manutention sur les différents sites du SGDSN, dans le cadre des déménagements et mouvements internes de mobiliers, 44 opérations de mise en configuration des salles de réunion et procédé à une opération de mise au rebut de 225 m³ d'encombrants ;
- l'atelier **reprographie-impressions**, très fortement sollicité dans des délais de réalisation souvent contraints, qui a produit plus de 2 millions de tirages et utilisé 18 tonnes de papier pour la réalisation des documents des conseils de défense et de sécurité et la production de nombreux rapports. Dans le cadre de la démarche de développement durable menée par le SGDSN, 200 cartouches de *toner* couleur et 30 bassines de récupérations de *toner* usagé ont été retraitées.
- le **centre de documentation**, qui propose un ensemble de ressources documentaires mises à la disposition des agents du SGDSN (presse nationale et internationale, ouvrages et revues thématiques) et offre également la possibilité d'emprunter des documents. En 2022, il a ainsi réalisé l'acquisition de 159 nouveaux ouvrages et opéré une sélection de 10 850 articles destinés principalement à la revue de presse et à la réalisation de veilles thématiques.
- le bureau du **courrier général**, qui a traité 27 000 courriers ;
- le bureau des **archives**, qui a mis en œuvre et décliné les évolutions législatives et réglementaires majeures sur la protection du secret et de la communicabilité des archives, intervenues en 2021. ◄

Questions à...

Philippe Decouais

Chef du service d'administration générale (SAG)

L'insertion de personnes en situation de handicap fait partie des priorités du Gouvernement. Comment le SGDSN se saisit-il de ce sujet ?

L'inclusion d'agents en situation de handicap est une priorité nationale que le SGDSN met progressivement en œuvre. Le handicap, visible ou invisible, est une réalité quotidienne pour de nombreuses personnes, qu'elles soient handicapées de naissance, atteintes d'une longue maladie ou qu'il s'agisse de militaires blessés. Pour souligner notre engagement, différentes initiatives ont été prises, dont la signature d'une convention de mécénat en faveur de la réinsertion par le sport des militaires blessés ou encore la participation au Duo Day.

De plus, la désignation récente d'une référente « handicap » va renforcer la coordination de l'ensemble de nos actions (suivi de la politique « handicap », information et communication sur les handicaps, dispositifs mobilisables...). Ainsi, dès la nomination de cette référente, des entretiens ont été menés pour orienter les personnes en situation de handicap et conseiller les équipes (*managers* et directions) dans l'accueil et l'intégration. Il reste à présent, avec le concours de chaque direction, à augmenter très significativement le taux d'emploi de personnes en situation de handicap. Des directives précises ont été données en ce sens par le secrétaire général, pour recruter et fidéliser les agents en situa-

tion de handicap, et inviter ceux qui n'auraient pas déclaré leur handicap à le faire, en toute confidentialité.

Comment la mise en place d'un SIRH participe-t-elle de l'évolution de la fonction RH et plus globalement du SGDSN ?

L'année 2022 a tout d'abord été l'occasion de sécuriser les SIRH existants et de permettre leur utilisation en télétravail grâce aux travaux de migration de plateforme, à l'automne, menés par l'OSIIC. Parallèlement, le projet de déploiement du SIRH interministériel RenoiRH a démarré en début d'année 2022 avec la constitution d'une équipe *ad hoc* composée d'une cheffe de projet interne et de prestataires mis à disposition par le centre interministériel de services informatiques relatifs aux ressources humaines (CISIRH).

L'adoption de ce nouvel outil a été l'occasion de nous interroger, dans un premier temps, sur la répartition des activités ayant trait aux ressources humaines au sein du SAG. Des ateliers menés en interne mais également avec la direction des services administratifs et financiers des services de la Première ministre, qui assure le rôle de direction ministérielle des ressources humaines, et avec le CISIRH, nous ont permis d'identifier une nouvelle organisation à mettre en place pour tirer pleinement parti des fonctionnalités offertes par ce SIRH. Ainsi, la double compétence « gestion administrative et préliquidation de la paie » est en cours de mise en place au sein de la division GRH du SAG. Le métier de gestionnaire des ressources humaines au sein des ministères s'inscrit dans une évolution globale, souhaitée par la direction générale de l'administration et de la fonction publique. Le SGDSN adopte ainsi les meilleures pratiques en termes de gestion administrative et de paie.

Un autre projet, mené depuis 2022 par la division « développement des RH » du SAG, va simplifier la vie des agents du SGDSN, de leurs *managers*, mais également des gestionnaires « ressources humaines ». Il s'agit du déploiement de l'application ESTEVE, utilisée par un grand nombre de ministères et établissements publics, qui permet de dématérialiser l'entretien d'évaluation annuel de chaque agent. Ce déploiement sera effectif pour la prochaine campagne en juin 2023.

Dans une période marquée par une nécessaire sobriété énergétique, quelles ont été les mesures prises par le SGDSN ?

Dans son allocution du 14 juillet 2022, le Président de la République rappelait l'importance de réduire les consommations d'énergie. En 2020 déjà, le Premier ministre avait annoncé 20 engagements pour des services publics écoresponsables. Le SGDSN s'est aussitôt engagé dans cette démarche de sobriété, en prenant en compte les contraintes imposées par nos différents bâtiments, dont ceux du site des Invalides, classé monument historique, et notre activité fortement liée au numérique.

Une chargée de mission « service public écoresponsable » a été nommée en qualité de référente sur les questions relatives à la politique environnementale du SGDSN. Elle travaille en étroite collaboration avec son homologue de la direction des services administratifs et financiers des SPM.
Plusieurs actions ont été engagées :

- une expérimentation portant sur les poubelles de tri a été mise en place à l'été 2022 et a connu un franc succès auprès des agents du SGDSN ;
- de plus, en lien avec l'OSIIC, un guide des écogestes a été élaboré et diffusé à l'ensemble des agents. Il retrace les bonnes pratiques relatives à l'environnement de travail (chauffage, climatisation, éclairage) décrites dans la circulaire de la Première ministre du 25 juillet 2022.

Ces actions viennent en complément de celles directement initiées par l'OSIIC (réduction du nombre de terminaux et recyclages des anciens équipements, optimisation de nos infrastructures d'hébergement) afin de tendre vers une sobriété numérique. ◄

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