PREMIÈRE
MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Rapport d'activité 2021

Rapport d'activité 2021

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
© Siren-Com/Wikicommons
© Gary Todd/Wikicommons
© État-major des Armées
© ESA
© Élysée

Sommaire

Édito

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

Après une année 2020 majoritairement consacrée à la gestion de la pandémie de Covid-19, 2021 aura été encore marquée par le traitement des divers aspects de la crise sanitaire.
Cependant, cette année aura aussi été celle des premiers retours d'expérience.

Le SGDSN s'est engagé dans un double travail de réforme des plans de gestion de crise et de réflexion sur une stratégie nationale de résilience. Ces travaux ont d'ailleurs été conclus ou ont largement avancé en 2022.

La pandémie n'a jamais interrompu les missions habituelles du SGDSN. Elle en a même intensifié certaines sur décision des conseils de défense et de sécurité nationale dont nous assurons le secrétariat.

Ces missions ont pris, ces dernières années, une dimension nouvelle : celle de la réponse aux menaces hybrides, c'est-à-dire aux attaques discrètes destinées à nuire à nos intérêts fondamentaux et à assurer à l'assaillant des gains sans s'exposer.

La cybersécurité a ainsi été une préoccupation croissante face à l'augmentation extrêmement rapide de la cyberdélinquance, diverse dans ses motivations, modes d'action et niveaux techniques. La pandémie a suscité une vigilance spécifique et accrue de la part de nos services envers un écosystème de santé (hôpitaux, collectivités publiques, opérateurs, etc) devenu plus critique. Grâce à l'action de l'ANSSI notamment, aucun service public n'a interrompu ses activités pour ce motif mais nous avons souvent évité de peu la catastrophe. Cet état de fait a incité le Gouvernement à intensifier les actions de cybersécurité conduites avec l'aide du plan d'investissement France Relance et de plus en plus de régions.

Les attaques d'origine étatique, espionnage ou sabotage, ont aussi largement augmenté contre des administrations, des organismes de service public ou des entreprises. L'ANSSI leur a été d'un précieux concours pour y remédier.

Autre menace hybride, la manipulation de l'information : le Président de la République a chargé le SGDSN de renforcer la vigilance et la protection du pays face au phénomène d'ingérence numérique étrangère. Pour ce faire, le 13 juillet 2021 a été créé le service connu sous le nom de VIGINUM. Le SGDSN est désormais en charge de la vigilance et la protection contre les ingérences numériques étrangères affectant le débat public. Il s'agit principalement de détecter et caractériser les phénomènes inauthentiques qui se manifestent sur les plateformes numériques et qui impliquent des acteurs étrangers. Dans le processus de création un soin particulier a été mis dans la consultation des principaux responsables parlementaires de toutes sensibilités, dans la prise en compte des remarques de la CNIL et du Conseil d'État, notamment pour asseoir le rôle du comité éthique et scientifique.

Enfin, toujours dans le domaine de la lutte contre les menaces hybrides, le SGDSN a veillé à la sécurité économique des opérateurs économiques, en liaison avec la direction générale des entreprises, et à la protection du patrimoine scientifique et technique.

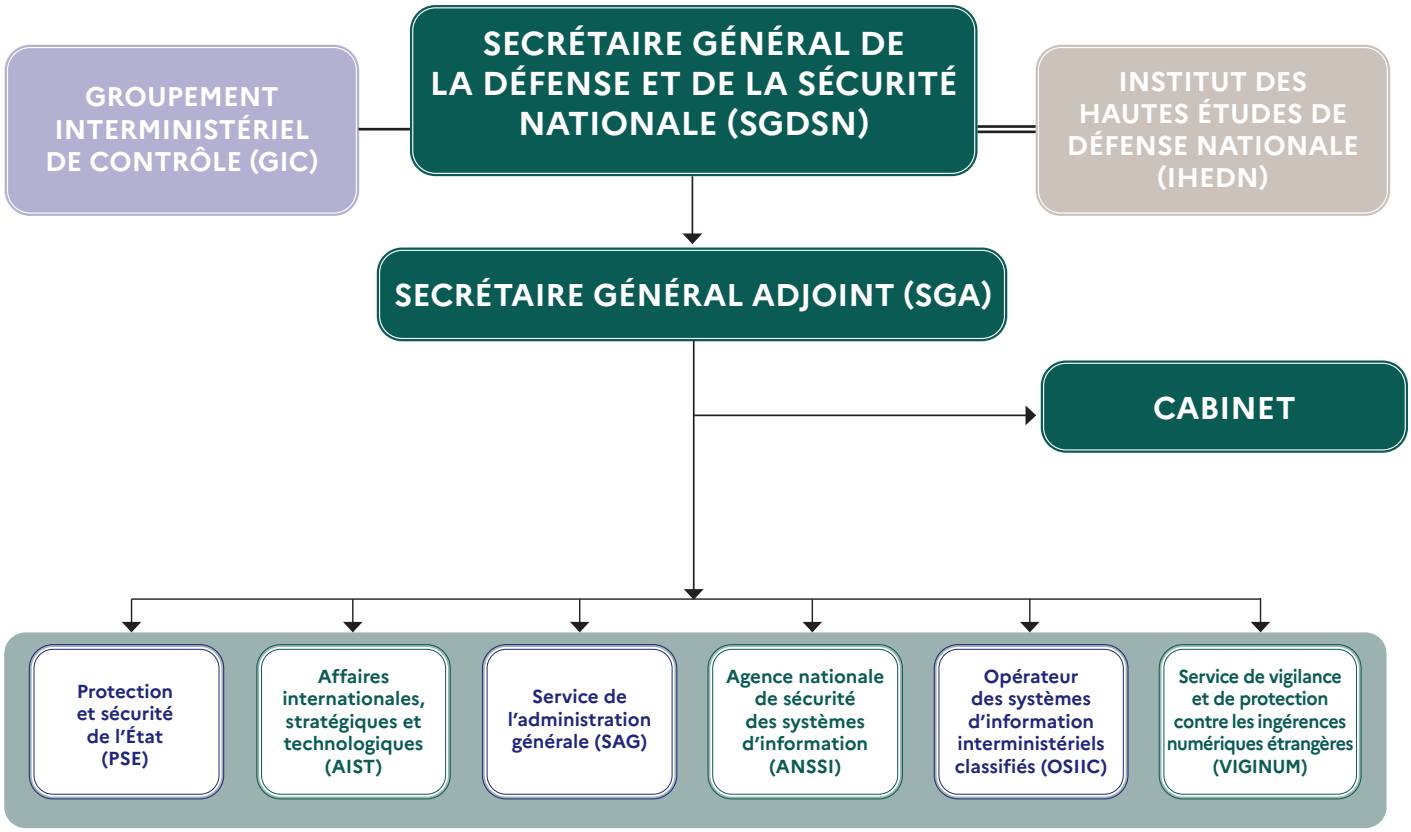
Le SGDSN a aussi mis à jour les règles de la protection du secret de la défense nationale. Il a par ailleurs répondu aux attentes du Parlement concernant le contrôle de l'exportation des matériels de guerre.

La coordination interministérielle, au service du Premier ministre, mission centrale du SGDSN, a ainsi trouvé une importance accrue en 2021, année d'une inquiétante évolution de toutes les conflictualités.

L'investissement des agents du SGDSN a été une nouvelle fois total et absolu, à quelque direction, service à compétence nationale ou service qu'ils appartiennent. Ce rapport d'activité est un hommage au travail qu'ils mènent conjointement avec leurs homologues des ministères. ◂

Organigramme

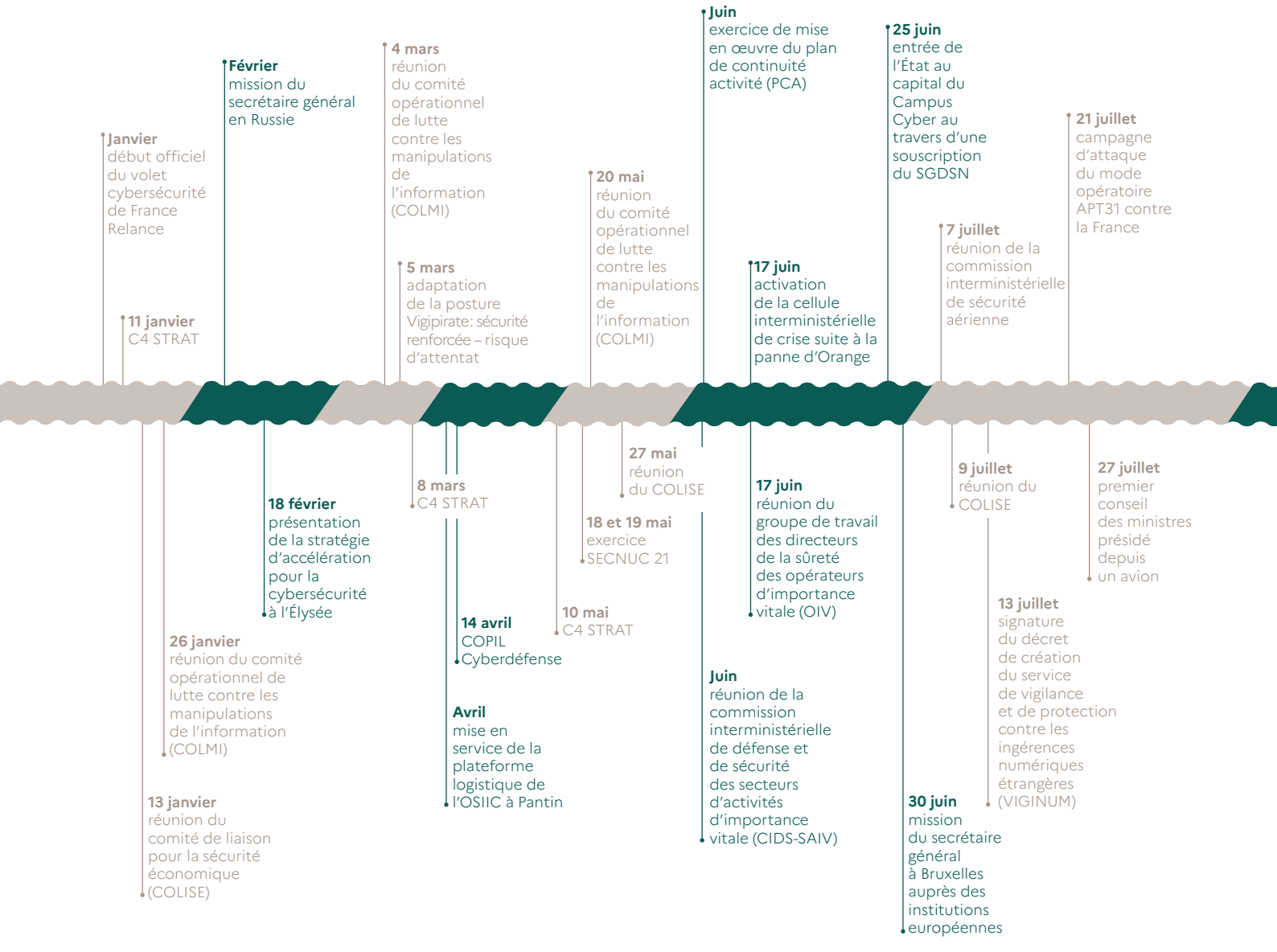
en date du 8 juin 2022

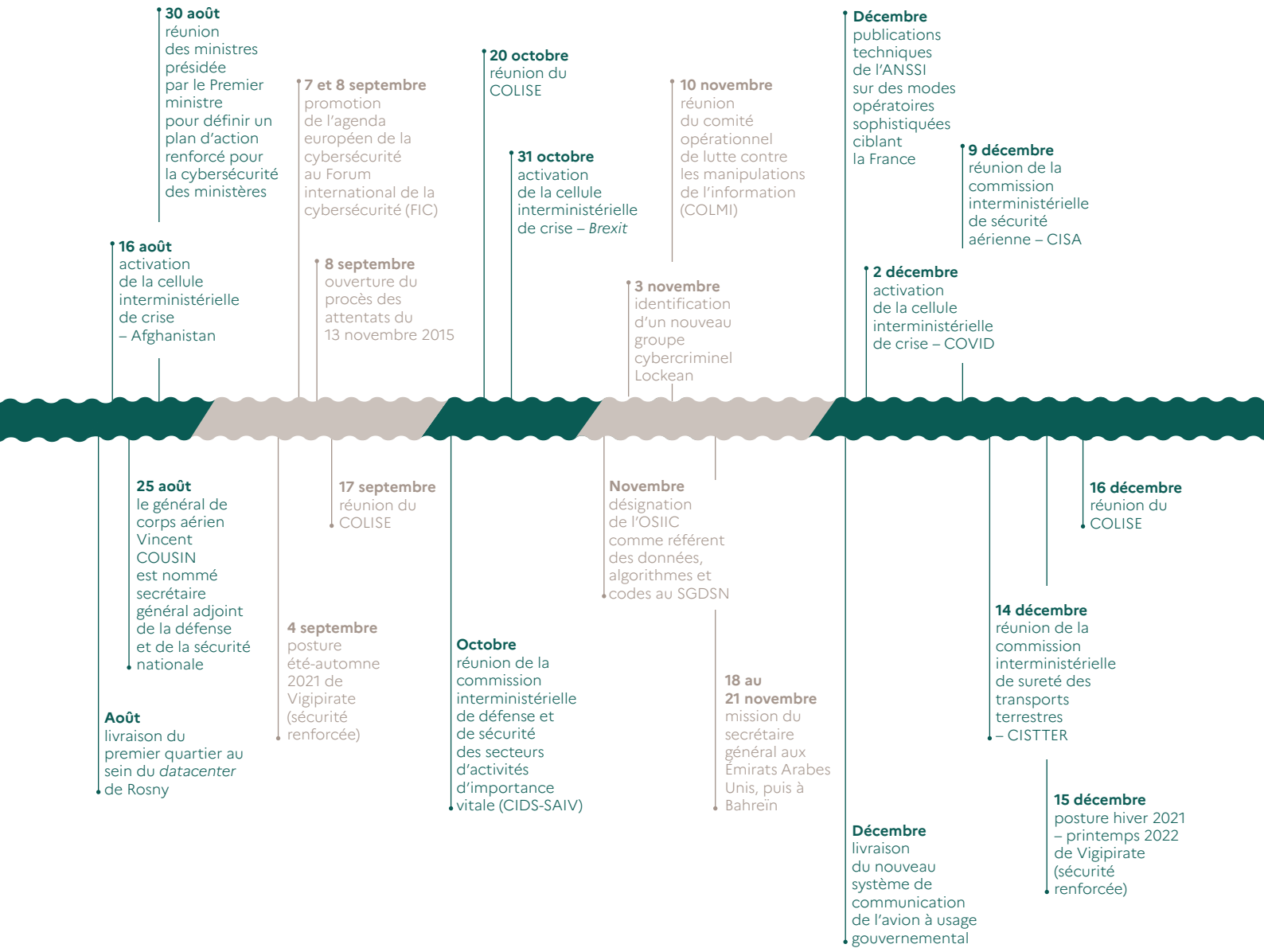


Effectifs au 31/12/2021

CAB :	14	ANSSI :	573
PSE :	58	OSIIC :	274
AIST :	52	GIC :	258
SAG :	60	VIGINUM :	17

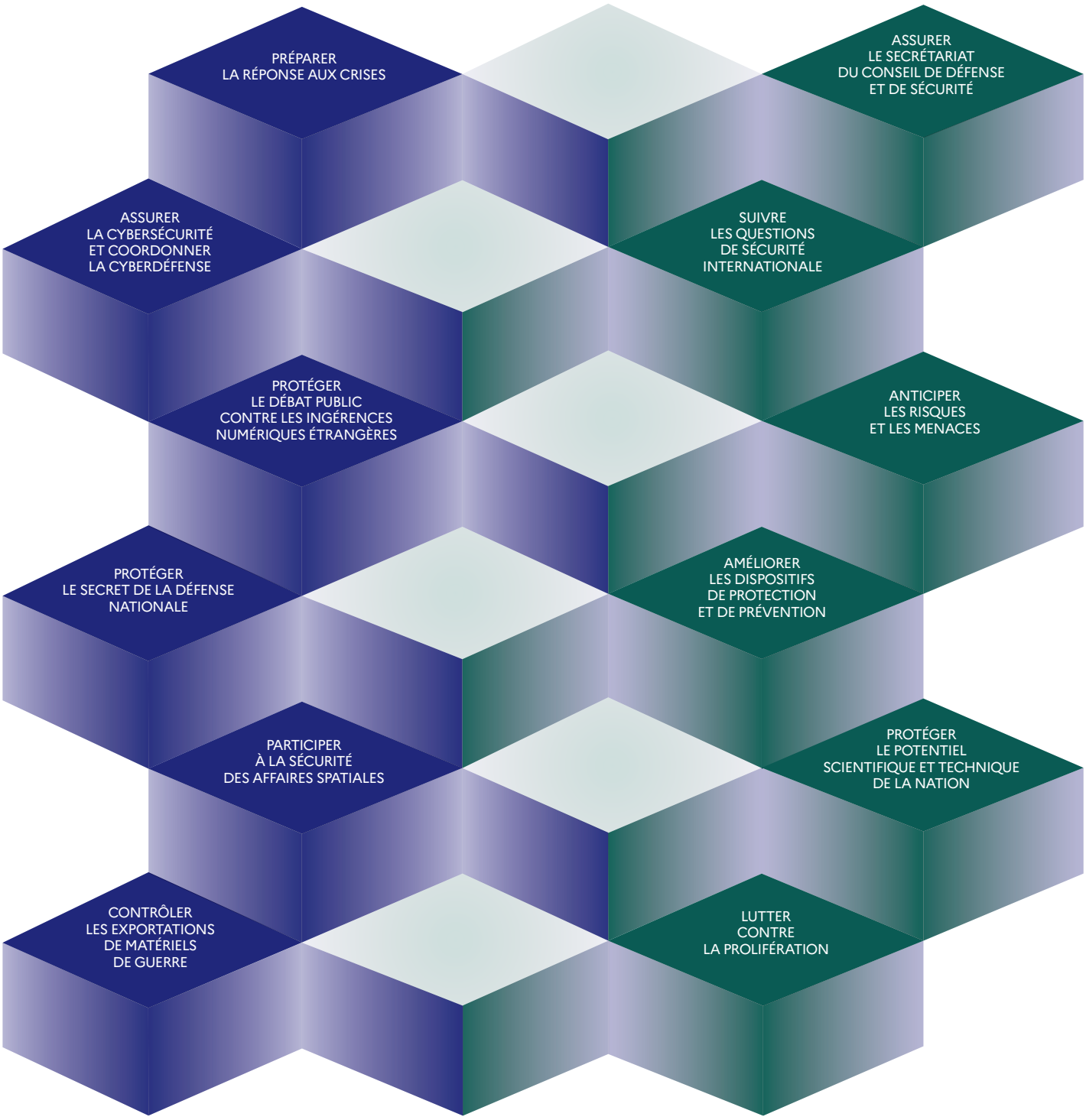
Éléments de chronologie 2021



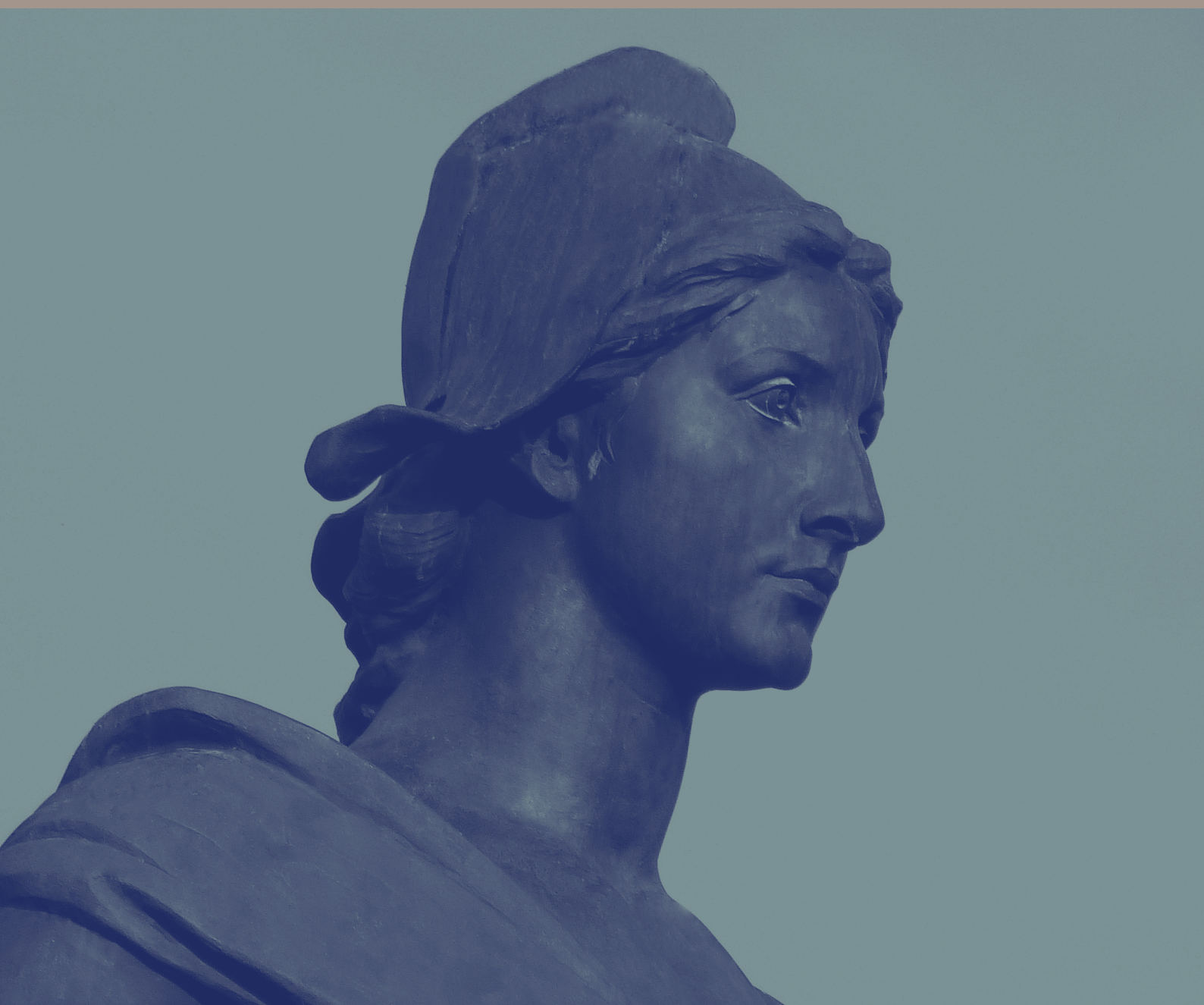


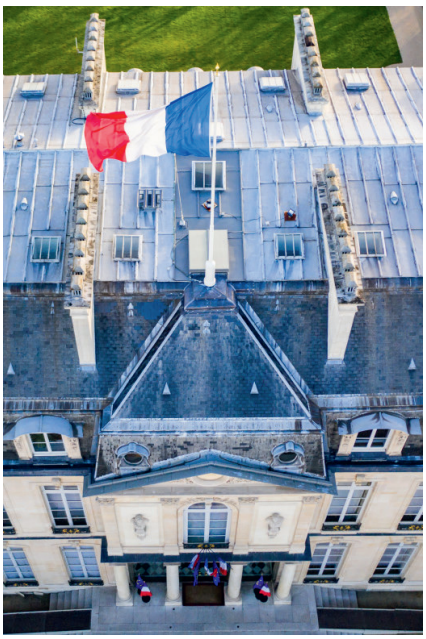
Octobre – juin 2021
3eme session de la professionnalisation des acteurs de la gestion de crise (PAGC)

Les grandes missions du SGDSN



Conseil de défense et de sécurité nationale





Outil de l'exercice par le Président de la République de ses prérogatives constitutionnelles, le conseil de défense a vu son niveau d'activité et son champ d'intervention varier au fil du temps. Réformé en 2009 d'après les orientations du *Livre blanc sur la défense et la sécurité nationale* de 2008, ses missions, sa composition et ses différentes formations sont définies par les articles R.*1122-1 du code de la défense.

Devenu « conseil de défense et de sécurité nationale » (CDSN), il réunit, sous la présidence du chef de l'État, le Premier ministre, le ministre de la défense, le ministre de l'intérieur, le ministre chargé de l'économie, le ministre chargé du budget, le ministre des affaires étrangères. D'autres ministres et responsables militaires et administratifs peuvent y assister sur convocation. Le Président peut en outre y convoquer toute personnalité en raison de sa compétence.

Le conseil de défense et de sécurité nationale définit les orientations en matière de programmation militaire, de dissuasion, de conduite des opérations extérieures, de planification des réponses aux crises majeures, de renseignement, de sécurité économique et énergétique, de programmation de sécurité intérieure concourant à la sécurité nationale et de lutte contre le terrorisme. Il en fixe les priorités, et propose des décisions au chef de l'État.

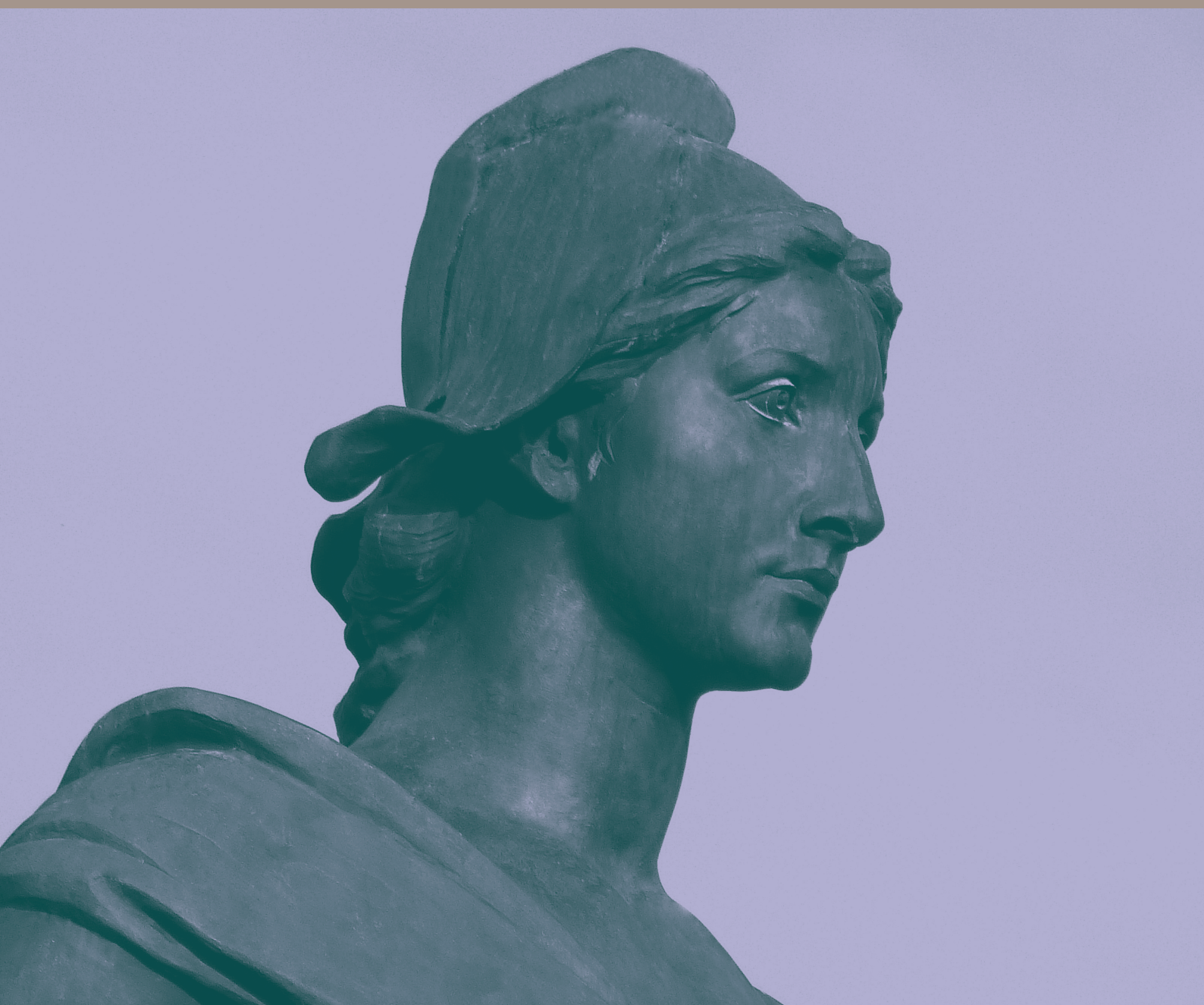
Le secrétariat du conseil de défense et de sécurité nationale, dans ses formations plénières, spécialisées et restreintes, est assuré par le secrétaire général de la défense et de la sécurité nationale.

À cette fin, le secrétaire général, en liaison avec l'état-major particulier du Président de la République et le cabinet du Premier ministre, constitue un dossier destiné aux participants. Pour ce faire, il arrête l'économie générale du dossier, il recueille et organise les notes fournies par les ministères. Il convoque et anime les réunions préparatoires. Il constitue et diffuse le dossier. À l'issue de la réunion du conseil, il assure l'ampliation et la diffusion du relevé de décisions. Il suit la mise en œuvre des décisions qui sont prises en conseil.

Depuis le mois de juillet 2016, le CDSN s'est réuni hebdomadairement. Ce rythme a été maintenu jusqu'au déclenchement de la pandémie due au Covid-19. Il a augmenté depuis. En 2021, le CDSN a été réuni à 82 reprises. La moitié de ces réunions a été consacrée à la gestion de la crise sanitaire. ◂

Le premier ancêtre du CDSN est constitué par le décret du 4 avril 1906 actant la création du Conseil supérieur de la défense nationale (CSDN). Il dispose d'un petit secrétariat non permanent commandé par un général de brigade. Peu utilisé pendant la Grande guerre, le CSDN est réactivé en 1920 et doté d'un secrétariat général permanent le 17 novembre 1921. À l'été 1943, un Comité de défense nationale est créé, coprésidé par les généraux Giraud et de Gaulle, puis par le seul Charles de Gaulle. Après-guerre, le secrétariat des conseils est successivement assuré par le Secrétariat du Comité de défense nationale (1943-1944), l'État-major de la défense nationale (1944-1949), l'état-major permanent civil et militaire de la présidence du Conseil (1949-1950) et le Secrétariat général permanent de la défense nationale (1950-1958). L'avènement de la Ve République modifie cette organisation. Le Comité de défense nationale est remplacé par un « conseil de défense » présidé par le Président de la République. Le secrétariat est assuré entre 1958 et 1962 par l'État-major général de la défense nationale, puis par le secrétariat général de la défense nationale de 1962 à 2009, date de la création du CDSN et du SGDSN tels que nous les connaissons désormais.◂

Préparer et réagir



Exercice de
cyno-détection
d'explosifs.

Élaborer une stratégie nationale de résilience

Le 16 juin 2021, le Premier ministre a donné mandat au SGDSN d'élaborer, avec l'ensemble des ministères, une stratégie nationale de résilience (SNR). Celle-ci vise à mieux préparer la France aux chocs futurs et à promouvoir notre définition du concept de résilience, notamment auprès des instances européennes et de l'OTAN.

Dans le domaine de la défense et de la sécurité nationale, la notion de résilience est définie dans le *Livre blanc sur la défense et la sécurité nationale* de 2008 comme « *la volonté et la capacité d'un pays, de la société et des pouvoirs publics à résister aux conséquences d'une agression ou d'une catastrophe majeure, puis à rétablir rapidement leur capacité de fonctionner normalement en tirant les leçons de la crise. Elle concerne non seulement les pouvoirs publics, mais encore les acteurs économiques et la société civile tout entière* ».

Dans un contexte marqué par le retour des conflits de haute intensité, la persistance de la menace terroriste, l'intensification et la succession rapide de crises majeures imputables à la survenance de risques sanitaires, financiers, sociaux et demain climatiques, il a été jugé indispensable de définir une stratégie de réponse globale. La résilience suppose tout d'abord une capacité à comprendre le monde qui nous entoure, sa complexité, les dynamiques qui le fragilisent et les crises qui le traversent. C'est l'objet de l'anticipation qui s'appuie d'abord sur une indépendance des analyses et se concrétise par les fertilisations croisées des réflexions. L'anticipation doit permettre d'oser des impensés afin de se prémunir de ruptures stratégiques.

Au-delà de considérations matérielles et capacitaires, la préparation à la survenance des crises relève d'une dimension humaine. Ainsi, la formation intellectuelle et le renforcement moral des citoyens y tiennent-ils une place prépondérante, car l'appareil d'État le plus solide ne résisterait pas à un effondrement moral de la population, qui demeure le centre de gravité de la Nation. Cela passe par une prise de conscience collective de la nécessité de préparer ceux qui la composent et par l'acquisition d'une culture commune de la gestion de crise. Chaque citoyen est donc un acteur de la résilience de la Nation.

La première phase d'élaboration de la SNR a permis d'identifier une soixantaine d'actions concrètes dont la mise à niveau des centres de crises centraux et déconcentrés, la constitution de stocks stratégiques, la mise en œuvre d'une communication adaptée à destination du citoyen et un renforcement humain des chaines de sécurité autour de trois objectifs stratégiques :

- préparer en profondeur l'État aux crises ;
- développer les capacités humaines et matérielles pour y faire face ;
- adapter la communication publique aux enjeux de la résilience.

En 2022, une nouvelle phase d'élaboration de la SNR visera à élargir la concertation aux représentants des collectivités territoriales et aux entreprises publiques et privées. Par ailleurs, l'analyse de l'étude comparative conduite au sein de l'Union européenne au cours de la PFUE permettra d'enrichir les réflexions nationales.

Refonte de la planification de sécurité nationale

Sur mandat du cabinet du Premier ministre du 12 février 2021, les travaux visant à la mise en place d'un plan de réponse aux crises sanitaires pandémiques ont été menés. Ces travaux s'articulent autour de deux axes : un plan générique et un volet capacitaire. Le SGDSN coordonne les différentes actions interministérielles. Ce plan sera validé en 2022. Il constituera un outil plus large que les plans « pandémie » qui existaient jusqu'alors et qui ciblaient des types particuliers de pathologies.

Plus largement, un grand travail de refonte de la planification interministérielle de sécurité nationale a été mené. Cette refonte vise à adopter une logique « tout risque » et à tenir ainsi compte des enseignements de la crise du Covid-19. Les travaux, lancés le 14 avril 2021, visent notamment à croiser 8 composantes transversales – organisation, anticipation, logistique, droit… – avec 12 domaines d'activités clefs – sécurisation, sanitaire, activités économiques, justice… Il s'agit, par ce biais, d'offrir des « briques » à assembler en fonction de la nature de la crise.

D'autres chantiers relatifs à la planification ont également été conduits. Ainsi, sur mandat du Premier ministre et en lien avec la coordination nationale du renseignement et de lutte contre le terrorisme (CNRLT), la direction de la protection et de la sécurité de l'État (PSE) du SGDSN a élaboré le nouveau Plan d'action contre le terrorisme 2021, dont l'exécution sera désormais suivie par la CNRLT. Parallèlement, le plan gouvernemental « crue de Seine » a été révisé, puis diffusé à la fin du mois de novembre à l'ensemble des ministères. Ce plan renforce la subsidiarité et donc le pilotage de ses objectifs par chacun des ministères.

En parallèle, PSE a débuté la rédaction de mémentos « opérationnels » relatifs au cadre juridique de la crise, à l'anticipation et à la logistique interministérielles. Ils permettront de compléter la documentation de planification par une approche plus opérationnelle.

Numériser la planification gouvernementale

En partenariat avec le ministère des armées, les travaux de réflexion autour du développement d'une plateforme numérique consacrée à la planification gouvernementale ont débuté au second semestre 2021. Ce projet associe l'OSIIC qui assurera le développement de l'outil ainsi que son maintien en condition. ◄

Réforme de la protection du secret

Une nouvelle version de l'instruction générale interministérielle n° 1300 (IGI1300) a été publiée le 9 août 2021. Elle remplace celle publiée en novembre 2020 et tire les conséquences de la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement. Pour le SGDSN, rédacteur de cette instruction, l'effort a principalement porté sur la bonne compréhension de la réglementation par les personnes chargées de la mettre en œuvre. Des actions de sensibilisations ont été réalisées, ainsi que des supports d'accompagnement.

Sur le plan des échanges d'informations avec nos partenaires, et ce à l'exception de quelques pays, tous les États partenaires ont été informés de la réforme française et de ses implications en la matière. Les nouvelles équivalences avec l'Union européenne et l'agence spatiale européenne sont effectives depuis le 1er juillet 2021 ; l'OTAN a donné son accord de principe aux nouvelles équivalences proposées, tout comme l'organisme conjoint de coopération en matière d'armement.

Développement des technologies de sécurité

Le centre national de certification en cyno-détection des explosifs (CYNODEX) a été créé par le décret n° 2021-1590 du 7 décembre 2021 sous la forme d'un service à compétence nationale du ministère de l'intérieur. Il a notamment pour mission de délivrer la certification technique pour la cyno-détection des explosifs. Celle-ci pourra être remise aux équipes cyno-techniques des services internes de sécurité et des entreprises privées de sécurité intervenant dans les services de transport public et dans les infrastructures ou gares de voyageurs. CYNODEX est localisé à Biscarosse, sur l'emprise de la direction générale de l'armement.

Dans le domaine NRBC, la composante PIRATOME a été intégrée au réseau national de laboratoires BIOTOX-PIRATOX. Ce réseau a pour mission de fournir aux autorités les éléments d'évaluation du risque nécessaires à la prise de décision, en cas de survenue d'un acte malveillant ou terroriste à composante nucléaire, radiologique, biologique et chimique.

Pour sa part, le plan national de réponse à un accident nucléaire et radiologique a été révisé. Par ailleurs, les travaux d'évaluation de la chaîne décisionnelle de haut niveau en cas d'événement nucléaire ou radiologique ont été lancés, avec la réalisation du premier exercice « Jardin d'Eden » le 24 juin 2021. ◄

Questions à...

Nicolas de Maistre

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

Pourriez-vous préciser le concept et les finalités de la stratégie nationale de résilience (SNR) ?

La succession de crises depuis près de 20 ans nous rappelle que nos sociétés évoluent dans un contexte d'incertitudes. La crise ponctuelle est devenue permanente. Les effets de la crise climatique, la guerre en Ukraine, ou encore les ruptures dans les chaînes logistiques nous conduisent à devoir réinterroger notre capacité collective à faire face en profondeur à des crises majeures et intersectorielles. C'est dans cette perspective que le SGDSN a reçu un mandat du Premier ministre pour coordonner l'élaboration d'une stratégie nationale de résilience.

Les travaux d'élaboration de cette stratégie, qui se sont déroulés dans des délais resserrés (cinq mois), visent à donner une cohérence d'ensemble à des objectifs et des actions souvent déjà portés par les ministères mais qui doivent être renforcés et suivis dans le temps au travers d'indicateurs. La résilience doit devenir une politique publique transversale qui irrigue les nombreuses autres politiques publiques et la vie toute entière de la Nation. Au-delà, cette démarche est aussi portée au niveau européen et atlantique.

La démarche a abouti à la définition d'une soixantaine d'actions couvrant un spectre qui va de la basse à la haute intensité. Elle a également mis en évidence un haut niveau d'engagement des ministères et permis de dresser un premier constat de nos forces et vulnérabilités, permettant d'en assurer un pilotage global. Un questionnaire adressé à l'ensemble des États membres de l'UE est venu compléter notre vision des dispositifs européens en matière de résilience.

La stratégie nationale de résilience a été validée par le cabinet du Premier ministre en mars 2022, conformément à l'échéance fixée. Nous avons proposé la création d'une commission interministérielle pour en assurer le suivi dans le temps. La prochaine étape doit nous conduire à étendre cette démarche auprès des collectivités territoriales et des différents opérateurs.

La nouvelle IGI 1300 est entrée en vigueur au mois de juillet 2021. Comment se passe cette transition ?

Je rappelle que cette réforme s'est construite autour du mot d'ordre « *mieux classifier pour mieux protéger* », la mesure la plus visible étant le passage de trois niveaux de classification (*Confidentiel Défense, Secret Défense* et *Très Secret Défense*) à deux niveaux (*Secret* et *Très Secret*).

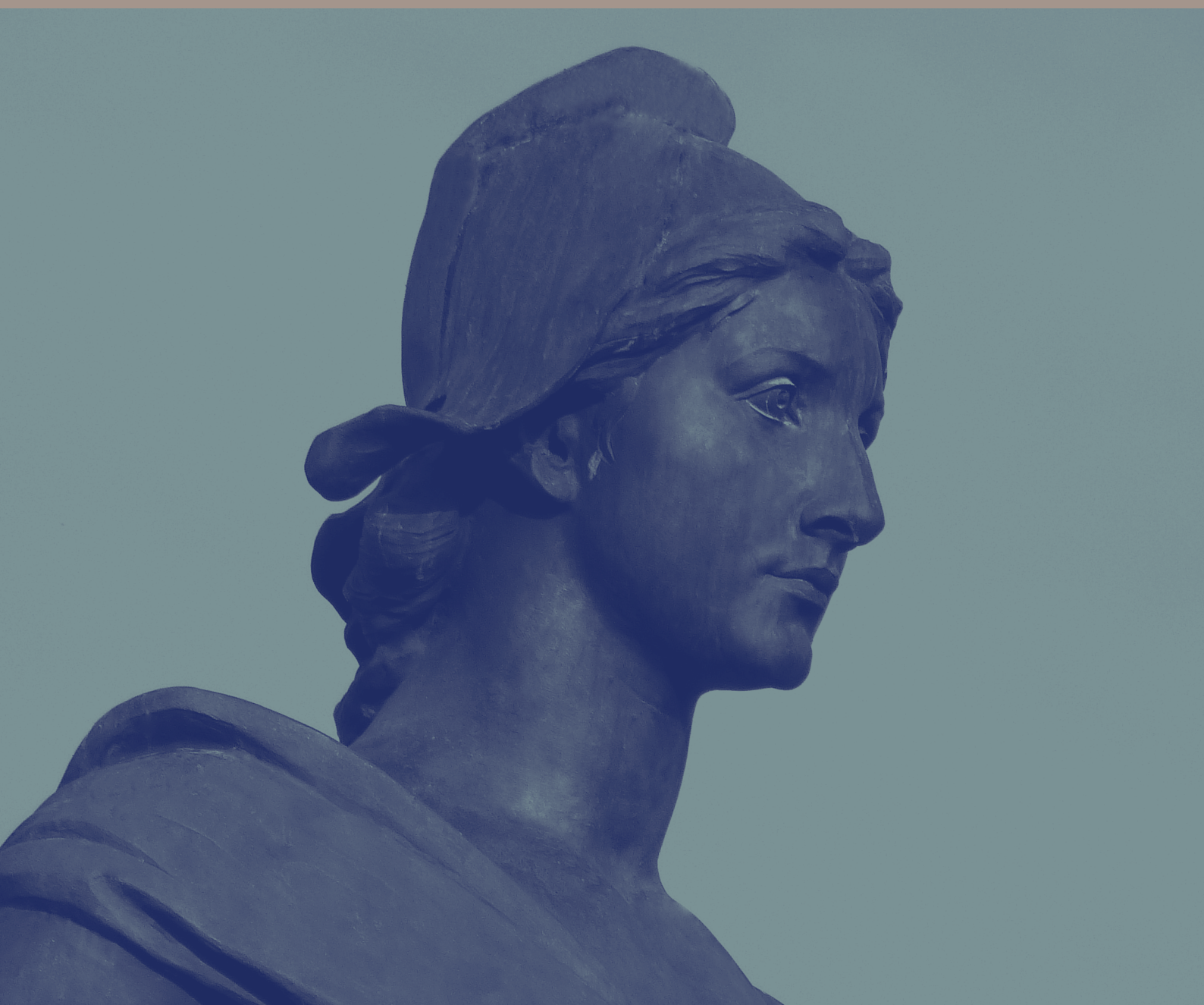
À ce stade, aucune difficulté majeure n'a été identifiée par les ministères, dans l'attente d'informations plus précises qui figureront dans le prochain rapport annuel sur la protection du secret qui sera remis à la Première ministre.

Si nous avons multiplié les actions de sensibilisations, nous avons, en parallèle, engagé des travaux pour professionnaliser la filière avec, notamment, la création d'un groupe de travail interministériel réunissant tous les fonctionnaires de sécurité et de défense (FSD) pour élaborer un référentiel de compétences des fonctions d'officier de sécurité qui sera repris par France compétences.

La réforme a aussi été relayée au plan international afin d'informer tous nos partenaires et les organisations internationales de ses conséquences en matière d'échange d'informations classifiées.

Au niveau bilatéral, c'est un travail de négociation de longue haleine qui s'est engagé pour mettre à jour les différents accords généraux de sécurité (AGS) avec nos principaux partenaires étrangers. À ce stade, une trentaine de projets d'amendement ont été transmis à nos partenaires sur la quarantaine d'accords à réviser.

Anticiper et contrôler



Anticipation interministérielle

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 anticiper les crises, à en atténuer les effets, à faciliter le retour à la normale. Elle fait l'objet d'une action spécifique dans la stratégie nationale de résilience (SNR). À cette fin, a été créé un comité interministériel d'anticipation (CIA) en septembre 2021, conformément au souhait du Président de la République de voir renforcer la capacité de l'État à anticiper les crises. Cette structure doit permettre de mettre en cohérence les dispositifs d'anticipation et de prospective de chacun des ministères, nécessitant un traitement interministériel, sur les sujets à forts enjeux, et proposer des recommandations opérationnelles ou une démarche de planification.

Des référents « anticipation » ont été désignés dans chacun des ministères et services concernés, afin de faciliter la coordination interministérielle. Le CIA se réunit deux fois par an au niveau des directeurs de cabinet, sous la présidence du SGDSN.

Lawfare

Sur mandat du cabinet du Premier ministre, le SGDSN a piloté en 2021 une étude interministérielle d'envergure sur le *lawfare*, entendu comme l'instrumentalisation du droit à notre détriment par nos compétiteurs stratégiques, principalement étatiques. Dans ce cadre, trois principales menaces ont été identifiées :

- l'instrumentalisation par certains États de leur propre droit, qui se traduit notamment par le développement de normes extraterritoriales ;
- l'utilisation stratégique des normes internationales ;
- le risque d'exploitation par des acteurs tiers de notre droit interne et de nos engagements européens.

Ces travaux ont permis de formuler des recommandations opérationnelles (ex. développer une extraterritorialité européenne voire nationale ; conduire une stratégie d'influence juridique) dont le SGDSN assurera le suivi. ◄

Stratégies hybrides

L'année 2021 a été marquée par l'accroissement de la menace russe sur le continent européen, en particulier dans les champs qualifiés d'« hybrides » dans la doctrine française, c'est-à-dire le cyberespace, le champ informationnel, le *lawfare*, les champs économiques, financiers et énergétiques et celui des opérations.

Les travaux interministériels dans ces domaines, animés par le SGDSN au travers d'un groupe de travail permanent qui s'est réuni 5 fois en 2021, ont abouti à la diffusion interministérielle, auprès des *think tanks* et de nos partenaires, d'un document de référence sur les stratégies hybrides de nos compétiteurs.

En outre, les réflexions sur les menaces hybrides étant particulièrement nombreuses aux niveaux international et européen, le SGDSN participe aux travaux du Centre d'excellence d'Helsinki sur les menaces hybrides. Il est également le point de contact national de la cellule de fusion hybride du Centre de situation et de renseignement de l'UE (*INTCEN*) et participe à l'élaboration des positions nationales qui sont portées au sein du groupe horizontal « menaces hybrides » (« *Enhancing Resilience and Countering Hybrid Threats* » – *ERCHT*) du Conseil de l'Union européenne. En 2021, dans le cadre de la préparation de la présidence française du Conseil de l'UE (PFUE) du premier semestre 2022, le groupe de travail interministériel sur les menaces hybrides a contribué à la préparation d'une feuille de route spécifique ainsi qu'à l'élaboration des priorités françaises pour le groupe *ERCHT*. Ces dernières s'inscrivent en cohérence avec les grandes priorités stratégiques de la PFUE, en particulier celle qui met en avant l'agenda de souveraineté européenne.

Missions internationales du secrétaire général

Le positionnement du SGDSN, auprès des hautes autorités politiques, et sa vision globale issue du travail interministériel, en font un interlocuteur utile pour nos partenaires, notamment lorsqu'ils possèdent des structures similaires (type *NSA*, *NSC*, etc.) et souhaitent aborder les questions de sécurité au sens large. Le SGDSN est aussi amené à porter des messages sur les questions de sécurité au sein des instances multinationales (UE, OTAN/CEPC), de formats particuliers de dialogue (Pakistan, Russie) ainsi que dans différents fora (*Forum* de Dakar, *Shangri-la Dialogue,* Conférence de Munich, etc.).

Le SGDSN, en tant qu'autorité nationale de sécurité et de cybersecurité, veille à ces questions tant en national qu'au niveau européen. Les failles de sécurité au niveau européen peuvent rapidement constituer des vulnérabilités au plan national. C'est ainsi qu'il a initié un plan de renforcement de la sécurité des institutions, agences et organes de l'Union européenne. Trois axes d'effort ont été promus : la diffusion d'une culture de la sécurité, la promotion d'une cybersecurité autonome, la protection des réseaux et informations classifiées. Dans ce cadre, deux textes ont été portés et font partie intégrante de la feuille de route du SGDSN pour la PFUE, sur la cybersecurité des institutions et sur la sécurité de l'information. Cette feuille de route conduira en partie les objectifs du SGDSN pour l'année 2022 en coordination avec le trio (République tchèque et Suède).

Protection du potentiel scientifique et technique de la Nation

Depuis deux ans, le SGDSN mène un travail interministériel de fond visant à faire évoluer le dispositif de protection du potentiel scientifique et technique de la nation (PPST) mis en place en 2012. Cette initiative répond à la demande du Président de la République de renforcer la lutte contre les ingérences étrangères. Deux projets de décrets destinés à optimiser le traitement des demandes d'accès en zone à régime restrictif (ZRR) par les ministères concernés ont été soumis à la Commission nationale de l'informatique et des libertés puis au Conseil d'État en 2021. Ils ont été publiés en mars 2022. Des travaux sont en cours pour adapter ce dispositif aux menaces actuelles, développer son caractère incitatif et affermir son volet de sécurité numérique. ►►►

Quantique

Dans le cadre de ses travaux de suivi des technologies de rupture d'intérêt pour la défense et la sécurité nationale, le SGDSN a réalisé, en lien avec les administrations concernées, un travail d'examen des technologies quantiques et de leurs implications. Il apparaît qu'à court terme (3 à 5 ans), les capteurs quantiques seront susceptibles d'introduire des ruptures majeures, notamment avec l'apparition de capteurs de champ et de navigation d'une grande précision. À plus long terme (15 à 20 ans), les ordinateurs quantiques, qui pourraient théoriquement offrir des performances de calcul bien supérieures à celles des ordinateurs classiques, permettraient de casser une partie des codes de cryptographie actuellement utilisés.◄

Élargissement à l'Espagne de l'accord franco-allemand sur les exportations d'armement

Signé le 17 septembre 2021, l'élargissement à l'Espagne de l'accord franco-allemand sur les exportations de matériels de guerre s'inscrit dans une volonté commune des trois partenaires de faciliter le développement de programmes de défense communs et de favoriser davantage la coopération entre leurs industries de défense.

L'accord trilatéral reprend les dispositions principales de l'accord franco-allemand, moyennant les adaptations nécessaires pour en permettre le fonctionnement à trois participants ou plus. Il fixe ainsi des règles et procédures de contrôle adaptées pour les exportations de produits liés à la défense afin de faciliter les transferts dans une logique de confiance mutuelle, et ce dans trois cas de figure : programmes intergouvernementaux, coopération industrielle, et sous-ensembles destinés à l'intégration dans un système d'arme avec une règle dite du *de minimis*.

La France assure la charge d'État dépositaire de cet accord multilatéral.◂

▸▸▸

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

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

La CIEEMG a instruit 7 800 demandes en 2021. Près de la moitié de ces demandes portent sur des modifications ou des prorogations de licences existantes. L'accroissement des demandes de prorogations, déjà constaté en 2020, s'est accentué en 2021.

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 2021, ces travaux ont notamment porté sur la préparation d'une nouvelle licence générale de transfert (LGT) destinée à simplifier certains transferts intra-européens. Ce texte réglementaire, publié au printemps 2022, facilitera la mise en œuvre des projets de coopération industrielle dans le domaine de l'armement financés sur des fonds européens.

À la suite des travaux de la commission des affaires étrangères de l'Assemblée nationale, le Premier ministre a souhaité renforcer l'information des parlementaires sur les exportations de matériels de guerre, sous la forme d'une communication annuelle devant les assemblées. Le SGDSN a préparé le décret n° 2021-885 du 2 juillet 2021 qui concrétise cette nouvelle pratique.

Au terme d'une longue négociation, le nouveau règlement européen 2021/821 sur le contrôle des exportations de biens à double usage est entré en vigueur le 9 septembre 2021. Ce règlement traite 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 « attrape-tout », en cas de violation des droits de l'Homme. Ce règlement accroît également les obligations de transparence des États membres, vise à mieux prendre en compte la question des biens intangibles et tend vers une meilleure harmonisation des systèmes de contrôle européens sur les biens à double usage.

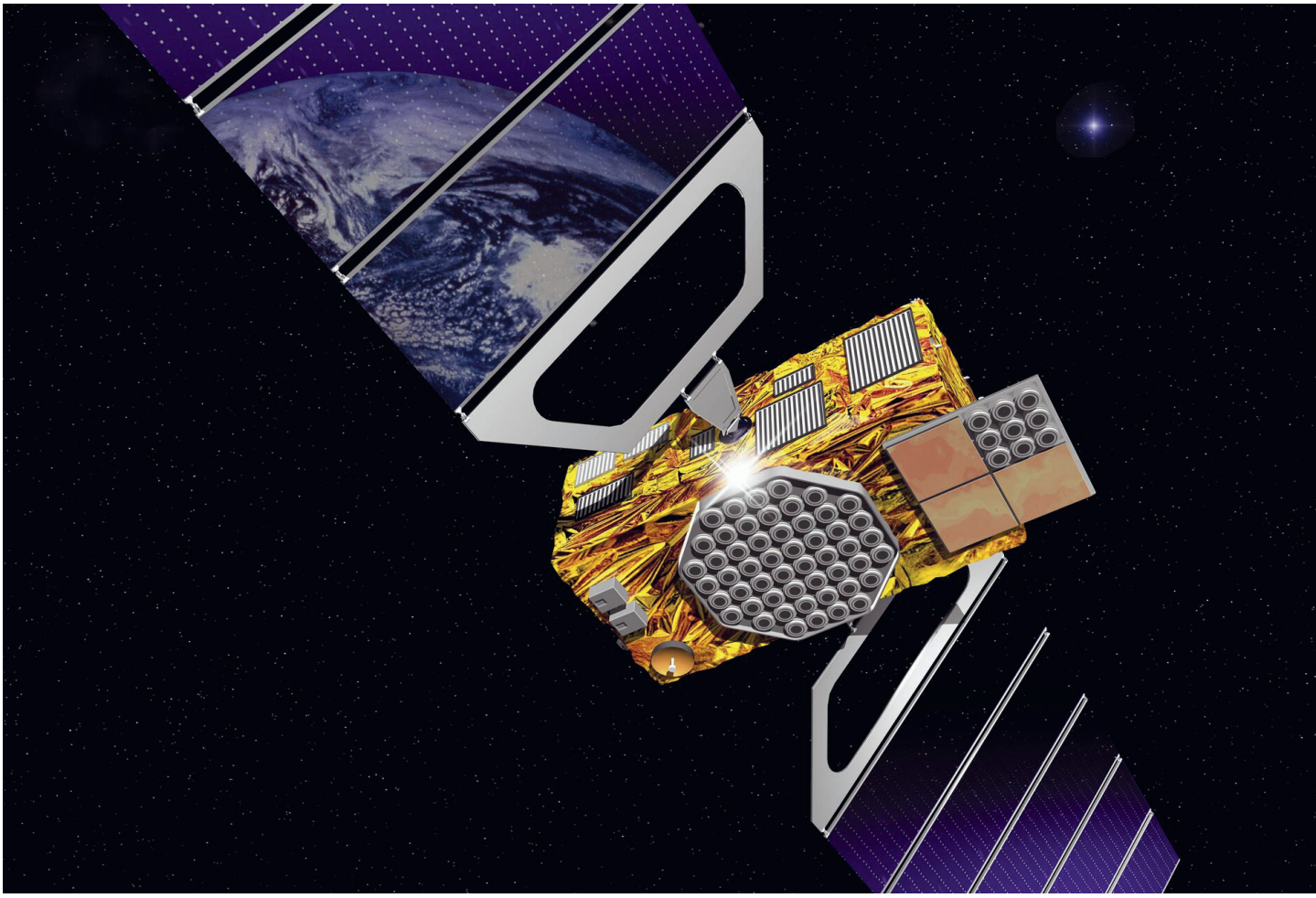
Participer à la sécurité dans les affaires spatiales

L'Union européenne conduit actuellement plusieurs programmes majeurs dans le domaine spatial : Galileo et Egnos pour le positionnement par satellites, Copernicus pour l'observation de la terre, GovSatCom pour la fourniture de capacités et de services de télécommunications au profit d'infrastructures critiques et enfin SSA (pour *Space Situational Awareness*) relatif à la surveillance de l'espace. La maîtrise de la sécurité des activités spatiales de l'Union européenne nécessite un dialogue soutenu avec les ministères, la Commission européenne et les États européens ou non. Dans la perspective de la présidence française de l'Union Européenne, le SGDSN a contribué à la définition des positions nationales sur ces sujets en particulier concernant le *Space Traffic Management* et la mise en application du nouveau règlement sur le programme spatial européen adopté en 2021.

En tant qu'autorité nationale responsable de la sécurité du signal protégé (*Public Regulated Service*) de Galileo, le SGDSN a poursuivi les activités de déploiement de ce système et endossé une responsabilité similaire concernant l'initiative GovSatCom.

Enfin, le SGDSN a participé aux travaux de modification de la loi sur les opérations spatiales en vue d'élargir le régime de déclaration des activités d'exploitation primaire de données d'origine spatiale. ◄

Système Galiléo



Questions à...

Jean-Hugues Simon-Michel

Directeur des affaires internationales, stratégiques et technologiques (AIST)

Selon vous, faut-il craindre pour l'avenir du financement de notre base industrielle et technologique de défense (BITD) ?

La France est dotée d'une industrie de défense capable de concevoir, produire et entretenir de manière autonome la majorité des équipements de nos armées. Néanmoins l'ensemble des acteurs concernés est soumis à des contraintes croissantes risquant de nuire, à terme, aux investissements dans le secteur de l'armement. On observe notamment une préoccupation grandissante des investisseurs pour les risques réputationnels, renforcée par le développement de critères extra-financiers au sein d'un corpus normatif européen et international toujours mouvant mais aussi par la pression de certaines organisations non gouvernementales. Le SGDSN a ainsi créé un groupe de travail interministériel d'anticipation, afin d'identifier les menaces et les vulnérabilités pesant sur la pérennité du financement de la BITD et l'accompagnement à l'exportation de cette industrie de haute technologie, en vue de proposer des mesures adaptées à ce nouvel environnement.

Quel est le rôle du SGDSN en matière de lutte contre la prolifération ?

Le SGDSN coordonne les actions de lutte contre la prolifération et la dissémination des biens et des technologies sensibles.

À cet égard, en matière de lutte contre la prolifération, la sous-direction non-prolifération, sciences et technologies (PST) du SGDSN coordonne les administrations mobilisées dans le cadre des actions d'entrave aux trafics des biens et technologies proliférants. Elle coordonne également les positions techniques françaises qui sont défendues dans les enceintes internationales traitant de contrôle des exportations sensibles telles que l'arrangement de Wassenaar (armes conventionnelles et biens et technologies à double usage), le *Missile Technology Export Control (MTCR), le Nuclear Supplier Group (NSG)* et le Groupe de l'Australie (armes chimiques et biologiques).

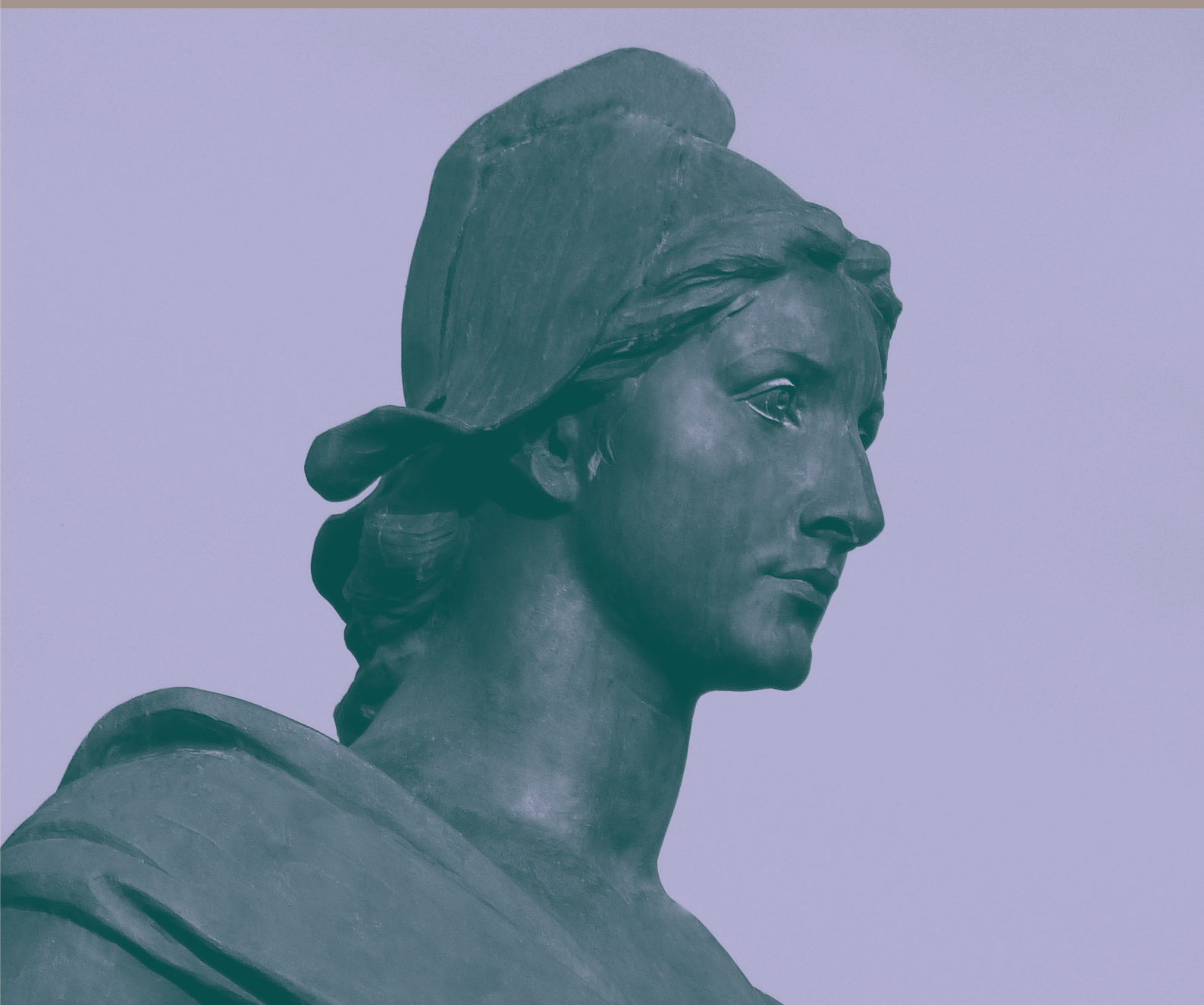
S'agissant de la protection des technologies sensibles et des savoir-faire associés, le SGDSN pilote le dispositif interministériel de protection du potentiel scientifique et technique de la Nation (PPST), qui s'appuie, notamment, sur la mise en place de zones à régime restrictif (ZRR). Ce dispositif vise à éviter des captations qui pourraient conduire à une prolifération d'armes de destruction massive, une dissémination d'armements conventionnels, un risque terroriste ou une atteinte à notre potentiel économique.

Enfin, le SGDSN intervient, à la demande des autorités et de manière ponctuelle, sur des sujets liés à la prolifération, le plus souvent aux frontières de problématiques techniques, économiques et géopolitiques.

Comment la nouvelle dynamique des activités spatiales que l'on nomme le *New Space* est-elle prise en compte par le SGDSN ?

Le nombre croissant de projets de lanceurs spatiaux privés doit nous conduire à définir de nouvelles mesures d'encadrement. La diffusion des technologies et des savoir-faire critiques constitue également un défi du fait des risques de prolifération. La multiplication des services fournis depuis l'espace, y compris par des acteurs privés toujours plus nombreux, nécessite la consolidation de règles permettant d'assurer la protection de nos intérêts. Ces services peuvent avoir une dimension commerciale dont l'usage doit être encadré comme nous le pratiquons déjà au niveau national pour les données d'observation de la Terre. Face à ces enjeux, le SGDSN va étoffer son organisation en vue de disposer au niveau interministériel de la capacité de relever ces défis au service de la Première ministre.

Accompagner et prévoir



Le service de l'administration générale (SAG) exerce les missions d'administration générale nécessaires à l'activité du SGDSN et des services à compétence nationale qui lui sont rattachés (ANSSI, OSIIC, VIGINUM) ainsi qu'à celle du groupement interministériel de contrôle. Concrètement :

- il assure la gestion de proximité des personnels militaires, la gestion de proximité et la paye des personnels civils titulaires ainsi que la gestion administrative et la paye des agents civils contractuels. Le SAG est chargé des modalités administratives et financières de recrutement. Il pilote la gestion des emplois et de la masse salariale ;
- il est chargé de la préparation, la programmation et du suivi de l'exécution du budget ainsi que de l'exécution des dépenses et des recettes. Il pilote le contrôle interne financier et s'assure de sa mise en œuvre ;
- il contribue à la définition et à la mise en œuvre de la stratégie ministérielle d'achat, établit la programmation des achats et assure la passation des marchés et contrats ;
- il programme, met en place et gère les moyens de fonctionnement et d'équipement ;
- il programme et conduit les opérations immobilières ;
- il met en œuvre les directives du secrétaire général en matière de sécurité interne au SGDSN ;
- il assiste le secrétaire général dans l'exercice de la tutelle de l'IHEDN.

Ressources humaines

Chaque année, le SGDSN, à la fois administration et opérateur de l'État, fait face au défi de la gestion d'une ressource humaine indispensable à la réussite de ses missions interministérielles. Avec une population constituée majoritairement d'agents de catégorie A, un taux de renouvellement annuel élevé et une forte diversité de statuts et d'origines, le SGDSN a poursuivi en 2021 une politique de ressources humaines dynamique et adaptée à l'évolution de ses missions.

L'augmentation continue des effectifs s'est poursuivie (+55 ETP en 2020 ; +62 ETP en 2021) et un nouveau service à compétence nationale, VIGINUM, a grossi les rangs du SGDSN à l'été 2021. Cette croissance, liée à l'extension des missions du SGDSN, rend d'autant plus crucial l'enjeu du recrutement, dans un contexte très concurrentiel. L'enrichissement du parcours professionnel des agents, au travers notamment d'un effort soutenu en matière de formation est également impératif.

Recrutement, formation, apprentissage, gestion des talents, valorisation des cursus des personnels, sont les principales lignes de force de la transformation RH, dont les premiers effets commencent à se faire sentir. Ce projet permettra, dès 2022, le déploiement d'un SIRH moderne autour duquel l'ensemble des processus RH vont être modernisés, avec un objectif de lisibilité, d'agilité et de flexibilité.

Enfin, le SGDSN poursuit son engagement en faveur de la diversité et de l'égalité femmes-hommes, recherchant les avantages opérationnels et sociétaux portés par la diversité des effectifs et la promotion de l'inclusion de tous les talents.

Finances et administration générale

Avec un budget de 312 millions d'euros en autorisations d'engagement et 284 millions d'euros en crédits de paiement confortant le SGDSN dans l'exercice de ses missions, l'année 2021 aura été plus particulièrement marquée par :

- la consolidation de l'OSIIC en tant que service à compétence nationale ;
- l'accompagnement de la création du nouveau service à compétence nationale, VIGINUM, qui a eu des incidences budgétaires qui se concrétisent en 2022, en lien avec sa montée en compétence et l'atteinte de sa cible emploi ;

- la mise en œuvre d'un volet du plan France Relance avec pour objectif d'accélérer la sécurisation des systèmes numériques de l'État et des territoires face aux risques numériques. L'enveloppe budgétaire initialement attribuée à l'ANSSI de 136 millions d'euros a fait l'objet d'un abondement complémentaire de 40 millions d'euros. Au total, ce seront donc 176 millions d'euros qui auront été engagés en 2021 et 2022, ce qui témoigne de la dynamique de dépenses portée par ce volet numérique, avec un écoulement des paiements prévu jusqu'en 2024 ;
- la réalisation d'un important travail de structuration et d'instrumentation des processus financiers avec la poursuite du déploiement des modules du systèmes d'information financier, en particulier de Chorus DT qui permet la numérisation du traitement des déplacements temporaires. Cet outil participe à la standardisation des processus de la chaîne de l'exécution financière, offrant ainsi un gain évident en robustesse et traçabilité.

En parallèle, la notification de 44 nouveaux marchés ainsi que l'établissement de plus de 2100 bons de commandes témoignent de la pleine mobilisation du service de l'administration générale durant l'année 2021, en dépit des aléas engendrés par la situation sanitaire. Le service de l'administration générale accompagne le SGDSN sur un large spectre de besoins, allant des travaux et de l'entretien immobilier des locaux jusqu'aux besoins en études et moyens en sécurité des systèmes d'information (SSI) ou encore la préparation des exercices interministériels.

Moyens généraux

Pour la division des moyens généraux, désormais rattachée à la sous-direction de l'administration générale et des finances, 2021 aura été un exercice particulièrement mobilisateur que ce soit à travers :

- la poursuite de la mise en œuvre du schéma directeur infrastructure (SDI) et la préparation du SDI 2021-2024, qui se seront traduites par la réalisation de nombreux projets immobiliers, notamment pour l'ANSSI : acquisition d'un bâtiment d'une superficie de 4440 m^2 au moyen de la formule de la vente en état futur d'achèvement à Rennes, prise à bail et accompagnement logistique dans l'installation au sein de plusieurs implantations nouvelles, notamment le Campus cyber ;
- une activité logistique qui aura quant à elle conduit à l'installation du nouveau service VIGINUM, à la réalisation de 800 prestations, dont une trentaine de déménagements, et – dans un contexte sanitaire toujours contraint – la gestion et la distribution de plus de 225 000 masques chirurgicaux ainsi que des produits de désinfection ;
- le bureau des impressions, dans des délais de réalisation souvent restreints, a de nouveau réussi à répondre au rythme imposé par les conseils de défense, les mesures COVID hebdomadaires et la production de nombreux rapports ;
- le centre de documentation dispose d'un nouvel espace au sein de l'Hôtel national des invalides et poursuit son activité de veille à travers la production de revues de presse et de recherches documentaires. Une convention a par ailleurs été signée avec le centre de documentation des SPM ;
- le courrier général aura géré près de 32 000 courriers (réception et envoi) pour 37 000 euros de coût annuel d'affranchissement ;
- le bureau archives, dont la participation à différents projets ponctuels, à la demande du Président de la République et ouvrant l'accès à certains documents, a fortement impacté l'activité. ◂

Questions à...

Philippe Decouais

Chef du service d'administration générale (SAG)

Pouvez-vous nous dire quels sont les premiers apports concrets de la transformation RH ?

La transformation RH ne bouleverse pas la fonction « ressources humaines », mais recherche des optimisations permettant de la rendre plus efficace et plus lisible pour les agents du SGDSN.

Un effort important a été engagé pour affirmer l'identité du SGDSN, dans un environnement métier très concurrentiel, afin d'attirer les talents et de mettre en lumière la qualité de vie au travail au sein de l'organisme. Pour fidéliser les talents, la mobilité interne au sein des directions est facilitée, et une politique ambitieuse de formation s'est structurée autour d'une charte qui engage l'administration et chaque agent.

Quelles sont les principales adaptations induites par la crise COVID ?

L'administration du SGDSN et de ses agents a fait face à l'enjeu de continuité d'activité en environnement COVID, en adaptant ses outils et ses modes de travail, en parfaite synergie avec la démarche de transformation numérique portée par l'OSIIC. Ainsi, nous avons contribué à encourager et faciliter le recours au télétravail et à la téléactivité (pour le personnel militaire), rendu certains services accessibles à distance et rendu la fonction « paie » beaucoup plus résiliente en permettant à nos agents de saisir les flux à distance dans Winpaie, sans devoir nécessairement se déplacer au bureau. Il n'y a ainsi eu aucune rupture de paie pendant toute la période COVID.

La fonction financière a également été mise sous tension, dans un contexte sanitaire contraint, pour garantir aux directions et entités du SGDSN un accompagnement de proximité sur tout le spectre de leurs besoins que ce soit à travers l'activité achat (44 nouveaux marchés et 2 105 bons de commandes), l'accompagnement de la création du nouveau service à compétence nationale, VIGINUM, ou encore l'exécution financière du plan France relance. Une attention particulière a été portée sur le délai de paiement de nos fournisseurs.

S'agissant des moyens généraux, la pandémie aura été également particulièrement mobilisatrice dans tous les domaines : à titre d'illustration, le bureau logistique a assuré la gestion et la distribution de plus de 225 000 masques chirurgicaux ainsi que des produits de désinfection.

Continuité, réactivité et adaptabilité auront ainsi été les principes directeurs du SAG sous l'empire de cette crise inédite jusque-là. Il s'agit désormais de capitaliser sur les enseignements que l'on peut en tirer pour poursuivre l'adaptation de nos procédures et nos modes de travail dans tous les domaines, au bénéfice de l'ensemble des directions et entités du secrétariat général.

Quels sont désormais les principaux enjeux à venir pour SAG ?

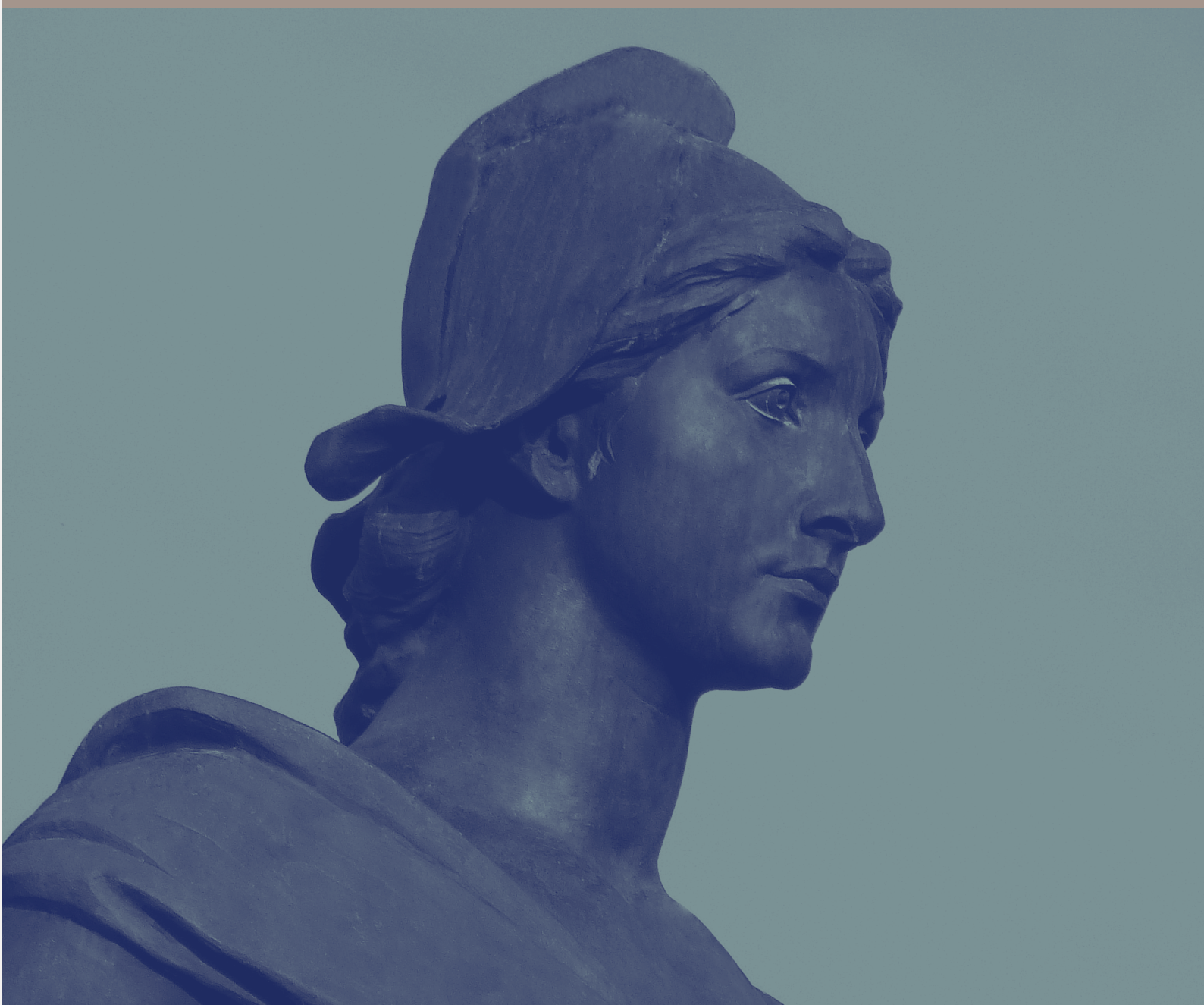
Il s'agit tout d'abord de poursuivre la démarche de transformation RH, en recherchant une amélioration permanente de « l'expérience collaborateur » *via* un SIRH moderne permettant à chaque agent d'accéder à son profil et de disposer d'un dossier unique numérisé.

Dans le domaine budgétaire et financier, la capacité de programmation et de pilotage du SGDSN sur ses ressources financières nécessite d'être consolidée pour répondre à l'enjeu porté par la rigidité croissante de son budget, qui ne lui laisse que peu de marges en gestion, dans le contexte de poursuite de la croissance « organique » du secrétariat général et de ses entités avec, en « toile de fond », la réforme récente du régime de responsabilité des gestionnaires publics.

Un autre enjeu de taille, pour les années à venir : l'immobilier et l'installation des effectifs en constante progression. L'occupation des locaux doit en effet être appréhendée à la lumière des ressources immobilières affectées ou pouvant être affectées au SGDSN mais aussi de leur disponibilité en fonction des travaux d'aménagement et de maintenance nécessaires. Aussi, afin d'anticiper et d'accompagner cette manœuvre, un schéma directeur pluriannuel d'occupation immobilière sera élaboré.

Enfin, SAG participe activement au renforcement de la fonction sécurité-sûreté du SGDSN dans le contexte de mise en œuvre de la nouvelle IGI 1300.

Protéger et convaincre



Mieux se préparer à faire face à une cyberattaque

Face à la croissance de la cybermenace, les organisations, entreprises et institutions doivent se préparer à faire face et apprendre à réagir pour maintenir leurs activités en cas d'attaque informatique. L'ANSSI a publié en 2021 une série de guides afin d'appréhender pas à pas la gestion de crise et ainsi faciliter la prise de décision :

- *Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique* – avec le Club des directeurs de sécurité des entreprises (CDSE) ;
- *Anticiper et gérer sa communication de crise cyber* - avec Cap'Com ;
- *Organiser un exercice de gestion de crise cyber*, réalisé en partenariat avec le Club de la continuité d'activité (CCA). ◄

Une menace qui continue de croitre

Alors que les années 2019 et 2020 avaient été marquées par une explosion des attaques par rançongiciels, cette menace s'est stabilisée, à un niveau néanmoins très élevé. En 2021, 203 attaques ont été traitées contre 192 en 2020. Ces attaques aux motivations crapuleuses, aux effets souvent très médiatisés, ne doivent cependant pas occulter l'existence de campagnes d'espionnage et de sabotage, particulièrement préoccupantes. Les opérations d'espionnage informatique restent en effet le principal type d'attaques menées par des attaquants « étatiques ». Leur traitement constitue l'essentiel des opérations de cyberdéfense conduites par l'ANSSI. Le ciblage d'infrastructures « critiques » est également une préoccupation majeure, notamment dans des moments de tensions géopolitiques exacerbées. De surcroît, l'ANSSI constate que de plus en plus d'actions de déstabilisation débutent par des attaques informatiques. Celles-ci ont pour objet de voler des documents qui pourront être ensuite divulgués, soit en l'état, soit préalablement truqués, pour déstabiliser une organisation, une personnalité ou encore un État.

L'ANSSI investit progressivement les nouveaux locaux du Campus Cyber.

Chiffres clés
(au 31/12/2021)

573
agents

21
millions d'euros de budget de fonctionnement et d'investissement

600
collectivités territoriales et établissements de santé bénéficiaires de parcours de cybersécurité dans le cadre de France Relance

105
établissements de santé désignés opérateurs de services essentiels (OSE)

17
opérations de cyberdéfense

Un effort important pour renforcer la cybersécurité des services publics en 2021

En 2021, sous l'impulsion du Premier ministre, les ministères se sont engagés dans un plan d'action visant à renforcer rapidement leur cybersécurité. Ce travail interministériel, lancé le 30 août 2021, a notamment permis d'assurer, au sein de chaque ministère, la prise en compte à haut niveau des risques de cybersécurité. Afin de suivre la progression du niveau de cybersécurité, les ministères se sont appuyés sur des outils automatisés de l'ANSSI. Les processus de traitement des alertes émises par l'ANSSI en cas d'existence de vulnérabilités ou de survenue d'incidents ont également été revus pour garantir leur prise en compte systématique par les ministères. Ces travaux, qui doivent impérativement se poursuivre en 2022, ont eu des effets très positifs sur la mobilisation des ministères.

L'année 2021 a permis de mettre en œuvre un dispositif d'ampleur pour sécuriser les services publics sur l'ensemble du territoire, au-delà des ministères. Des collectivités territoriales, des établissements de santé et des organismes publics ont pu bénéficier d'un accompagnement humain et technique pour renforcer rapidement et significativement leur niveau de cybersécurité. Ce sont ainsi 600 entités qui ont pu s'engager dans ce dispositif en 2021.

Par ailleurs, afin de démultiplier la capacité de réponse aux incidents de cybersécurité et protéger le tissu économique et social français, la création de centres régionaux de réponse à incidents de cybersécurité a été engagée au sein des régions, en liaison avec les préfets. En 2021, 7 régions se sont lancées dans la construction d'un tel centre : Bourgogne Franche-Comté, Centre Val de Loire, Corse, Grand Est, Normandie, Nouvelle Aquitaine et Sud – Provence Alpes Côte d'Azur. Les *CSIRT* régionaux travailleront au service des entreprises, collectivités et associations locales pour les sensibiliser et les former aux bonnes pratiques, recevoir et qualifier leurs signalements d'incident, mettre en relation les victimes avec les structures adaptées pour les accompagner dans la résolution de l'incident. Ces structures regroupent les prestataires locaux de réponse à incident, qualifiés par l'ANSSI ou labellisés « ExpertCyber » par cybermalveillance.gouv.fr, le *CERT-FR* – centre national de réponse à incidents au sein de l'ANSSI, les services de police et de gendarmerie, auprès desquels les dépôts de plainte seront encouragés.

Le plan France Relance vise notamment à renforcer la cybersécurité des acteurs français.

Préparatifs pour l'ouverture de deux nouvelles implantations de l'ANSSI

En 2022 et 2023, l'ANSSI ouvrira deux nouvelles implantations : l'une au sein du Campus Cyber à Paris-La Défense et la seconde à Rennes.

L'antenne de Rennes, à proximité des services du ministère des armées, permettra d'approfondir les synergies étatiques. L'ouverture du site aura lieu au premier semestre 2023 et permettra d'accueillir 200 agents. Plus spécifiquement, les missions qui y seront menées s'articuleront autour de la connaissance de la menace en partenariat avec les acteurs institutionnels de la cyberdéfense et le renforcement des capacités de détection des cyberattaques. Le Campus Cyber vise, quant à lui, à faciliter la structuration d'un écosystème français de la cybersécurité par la création de synergies entre les acteurs publics, économiques, de la recherche et de l'éducation. Le site accueillera des agents dès le premier trimestre 2022 et verra notamment s'installer une nouvelle division de l'ANSSI « industrie et technologies », dont la mission sera de construire un lien pérenne avec l'écosystème privé.

Tout au long de l'année 2021, l'ANSSI, avec l'appui du SGDSN, a mené les travaux administratifs et techniques pour acquérir et louer ces implantations. Des agents de l'ANSSI ont également pris en charge la préfiguration de ces nouveaux locaux : certains d'entre eux ont déjà déménagé à Rennes où ils sont hébergés par le ministère des armées dans l'attente de la livraison du bâtiment de l'ANSSI. ◂

Questions à...

Guillaume Poupard

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

Quels ont été les principaux défis pour l'ANSSI en 2021 selon vous ?

En 2021, les rançongiciels ont encore été très visibles, car ils causent des dommages immédiats sur toutes les organisations, paralysant leurs activités et ce, parfois pendant plusieurs semaines. Cependant, ces cyberattaques génèrent un biais important, car elles masquent d'autres cyberattaques moins spectaculaires, mais qui mobilisent très fortement les équipes de l'ANSSI. Il s'agit des cyberattaques à des fins d'espionnage qui représentent la très grande majorité des opérations de cyberdéfense de l'agence. Être en capacité de répondre à tout type d'incident de cybersécurité, qu'il soit d'origine criminelle, étatique ou inconnue, est un vrai défi qui impose à l'ANSSI de se maintenir au niveau technique des attaquants, de bien les connaitre, de savoir les détecter et de pouvoir réparer les systèmes d'information attaqués.

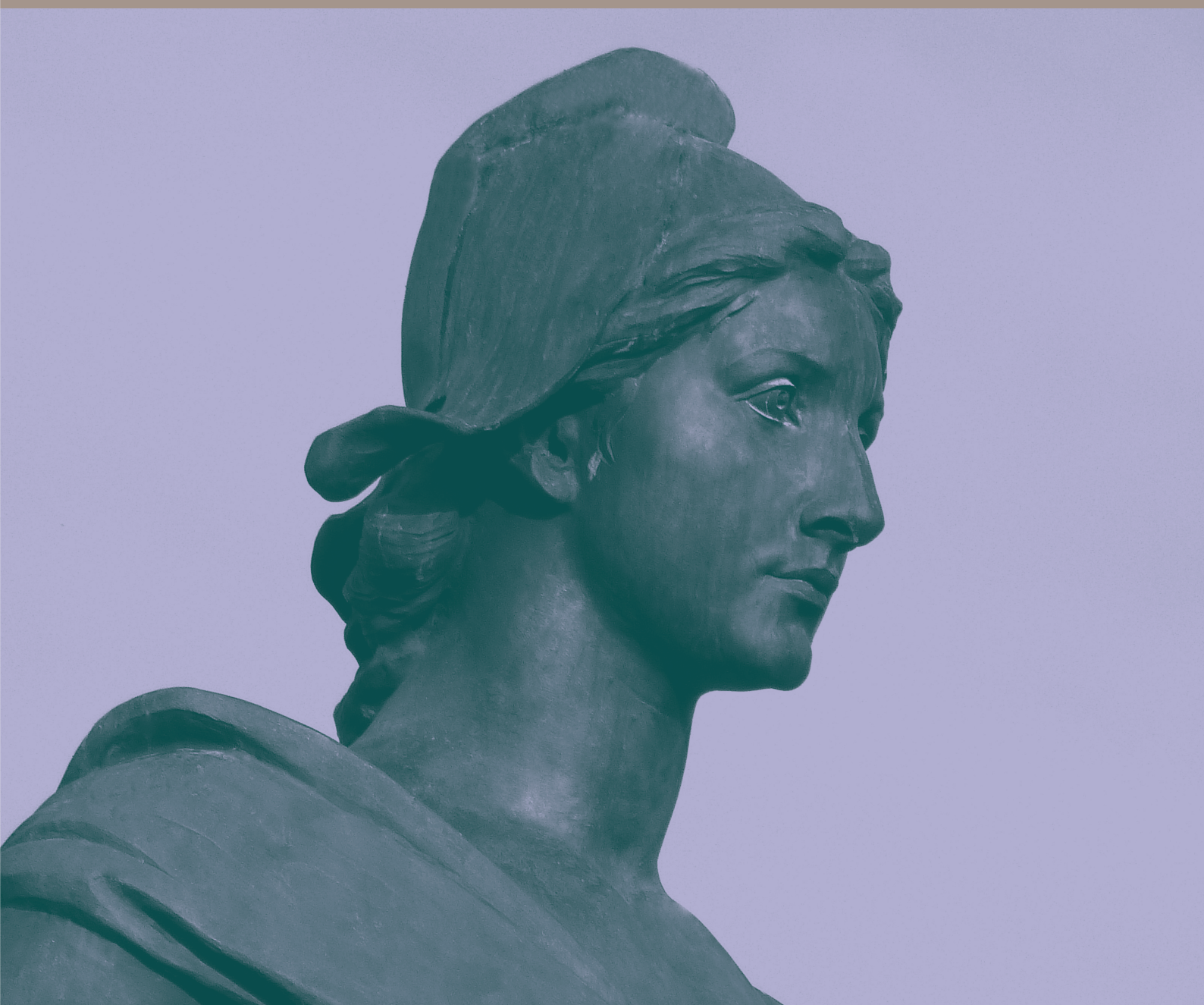
Le deuxième défi qui a marqué l'année est celui de l'offre des solutions que nous apportons aux organisations qui souhaitent se sécuriser. Renforcer sa cybersécurité demande du temps, de l'argent et des compétences dont toutes nos administrations et entreprises ne disposent pas. Il faut donc les convaincre d'investir dans ce domaine et leur donner des outils pour les accompagner dans ces travaux. C'est pour cette raison que, encore en 2021, nous avons publié de nombreux guides, puissamment aidé divers projets numériques de l'État, développé des services de cybersécurité automatisés ou encore travaillé à l'élaboration d'indicateurs fiables pour permettre un meilleur pilotage de la cybersécurité d'une entité.

Enfin, l'ampleur de la cybermenace et la vulnérabilité persistante des outils numériques obligent l'ANSSI à identifier des relais divers pour démultiplier son action. Pour cela, nous qualifions des prestataires de services de cybersécurité pour attester de leurs compétences, nous développons des formations en cybersécurité et nous travaillons étroitement avec les autres services de l'État qui disposent d'une compétence pour muscler notre réponse face aux agressions que connait la France. Malgré ces avancées, faire passer notre action à l'échelle idoine demeure un vrai défi.

Lors du premier semestre 2022, la France a exercé la présidence de l'Union européenne. Quels ont été les enjeux de la préparation de cette séquence pour l'ANSSI ?

L'année 2021 a résolument été tournée vers l'avenir, notamment afin de préparer la présidence française de l'Union européenne (PFUE). Cette présidence est une véritable occasion de renforcer la cybersécurité européenne. Cela a donc nécessité des préparatifs importants tout au long de l'année 2021 pour identifier les priorités, appréhender le programme de travail de l'UE dans le domaine de la cyberdéfense et garantir les meilleures conditions possibles pour la présidence. La révision de la directive NIS, la cybersécurité des institutions européennes, le développement d'un tissu industriel de confiance et la solidarité européenne en cas de crise majeure sont à ce titre des priorités qu'il faudra concrétiser durant cette présidence.

Transformer et développer



L'année 2021 a été la première année d'exercice complète de l'opérateur des systèmes d'information interministériels classifiés (OSIIC), créé le 1er juillet 2021. Son activité s'est structurée autour de trois axes d'effort majeurs : la réponse à des besoins opérationnels particulièrement prégnants, la poursuite de la consolidation de l'opérateur, et enfin la conduite de chantiers majeurs, pierres angulaires d'une offre de services rénovée.

Adapter l'offre de service proposée au SGDSN

L'OSIIC a fortement adapté l'offre numérique qu'il fournit au SGDSN, pour répondre au besoin de télétravail ou de fonctionnement distanciel. Ainsi, le déploiement d'une nouvelle solution d'ordinateur portable au niveau de sécurité Diffusion Restreinte, dont le développement avait débuté en septembre 2020, a été lancé selon un calendrier accéléré en mars 2021, pour faire face au rebond épidémique, et généralisé dans l'année à l'ensemble des agents du SGDSN. Cette évolution s'est accompagnée d'un travail de fond pour basculer les applications et usages qui le pouvaient depuis les réseaux de travail historiques du SGDSN, classifiés donc non accessibles à distance, vers le nouveau réseau Extranet accessible en mobilité. Un travail significatif a également été mené à bien pour permettre aux agents du SGDSN d'accéder aux solutions interministérielles de visioconférence, sans compromettre les conditions de sécurité spécifiques à leurs métiers.

Apportant de réels gains d'efficacité, mais aussi et surtout une capacité à fonctionner durablement « hors les murs », ces solutions contribuent ainsi à la résilience du SGDSN face à différents scénarios de crise, et ont joué un rôle central dans l'exercice « Plan de continuité d'activité » réalisé à ce titre en juin 2021. Elles sont également un facteur clé dans la capacité du SGDSN à fonctionner sur un nombre croissant de sites géographiques (VIGINUM, Campus Cyber, extension de l'ANSSI à Rennes) sans perte d'efficacité et de coordination.

Transformer l'OSIIC

L'OSIIC a poursuivi au cours de l'année le travail interne de consolidation et d'optimisation engagé lors de sa création en 2020. Il a ainsi déployé pour la première fois les outils de pilotage stratégique et budgétaire élaborés à cette occasion, tout en renforçant ses moyens humains et en développant ses fonctions de soutien interne en relai du service de l'administration générale.

L'opérateur a par ailleurs conduit plusieurs ajustements de son organisation, tirant le bilan de ses premiers mois de fonctionnement, selon trois axes principaux :

- une refonte complète de son organisation logistique, adossée à une plateforme logistique rénovée à Pantin, offrant des gains majeurs tant en matière d'efficacité que de bonne gestion des stocks ;
- une adaptation de son organisation pour le pilotage de projets numériques, favorisant la cohérence et l'adaptation au besoin utilisateur ;
- une amélioration des structures et processus mis en place pour le traitement des demandes des bénéficiaires, avec la création d'un centre de mise en œuvre unifié.

L'OSIIC a également renforcé sa coopération avec les ministères sur le déploiement et le soutien de ses systèmes d'information interministériels classifiés, en élaborant notamment plusieurs conventions bilatérales, et en lançant un projet de « hubs régionaux ».

Projet COMGOUV-NG

Le projet de refonte des moyens de communication de l'avion à usage gouvernemental long courrier a été mené à terme dans les délais prévus, malgré de nombreux retards initiaux dus à l'impact de la crise sanitaire sur différents fournisseurs. L'avion rénové, livré fin décembre 2021, dispose ainsi de capacités de communication renforcées, et d'une véritable extension à bord des systèmes de communication classifiés que l'OSIIC fournit par ailleurs au Gouvernement.

Ce succès n'a été possible qu'au prix d'une forte mobilisation des équipes de l'OSIIC, notamment lors des deux mois d'immobilisation de l'appareil sur l'aéroport de Mérignac. Il a été aussi l'occasion d'une coopération très étroite avec les personnels de la DGA, de l'Armée de l'Air, et des industriels Thales et Sabena, également mobilisés par ce défi collectif.

COMGOUV

Dans le cadre de leurs déplacements, les très hautes autorités de l'État ont besoin de disposer de toute la panoplie des services numériques, en tout temps, en tous lieux. Le programme d'armement COMGOUV-NG contribue directement à la continuité de service pendant les déplacements avec l'avion à usage gouvernemental (AUG). Ce programme, prioritaire pour l'OSIIC et le SGDSN, est le 3e programme déployé, après un cycle de plus de 10 ans, COMGOUV 1 ayant débuté en octobre 2010.

D'un point de vue système numérique, la grande nouveauté de COMGOUV-NG est la segmentation en deux parties inter-connectées, l'une sous la responsabilité de Thales, l'autre sous la responsabilité de l'OSIIC. L'enjeu est de pouvoir proposer à bord de l'AUG l'ensemble des services numériques étatiques.

En décembre 2021, les équipes de l'OSIIC sont entrées dans la dernière phase de ce programme qui consiste à tester les équipements et services de télécommunication sécurisée mis en place dans l'avion à usage gouvernemental (AUG).

Pour relever ce défi, toutes les composantes de l'OSIIC ont été engagées afin d'offrir un service de bout en bout. Le résultat présenté à l'État-major particulier (EMP) du Président de la République a nécessité plus de trois années de travail : phases de conception et d'architecture, puis de réalisation, d'intégration et de tests techniques, jusqu'aux tests fonctionnels. » ◄

Mise en service du nouveau *datacenter*

L'OSIIC a repris à sa création l'exploitation du *datacenter* hautement sécurisé mis en place par l'ANSSI et le ministère de l'intérieur, au sein du fort de Rosny. Un cap majeur a été franchi dans la valorisation de celui-ci en 2021, avec le déploiement d'un socle d'hébergement à l'état de l'art pour les systèmes d'information non classifiés de l'OSIIC, et la migration dans ce *datacenter* des premières applications. Cette migration se poursuivra en 2022 et devrait offrir d'importants gains de fiabilité et de souplesse d'emploi. Elle préfigure une refonte en profondeur des systèmes d'information classifiés de l'OSIIC, au sein de ce même *datacenter*. ◄

Chiffres clés
(au 31/12/2021)

1610
c'est le nombre d'équipements OSIRIS & HORUS déployés au 31 décembre 2021, dont

756
déployés en 2021 (soit 47 % du parc)

21
c'est le nombre de voyages officiels réalisés en 2021 par l'équipe COMTHAIE (communication des très hautes autorités de l'État)

60
c'est le nombre d'équivalant temps plein (ETP) mobilisé pour le programme COMGOUV-NG

Questions à...

Vincent Strubel

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

Comment l'OSIIC a-t-il été impliqué dans la transformation numérique du SGDSN ?

Le pilotage du projet de transformation numérique du SGDSN a été confié à l'OSIIC à compter de mars 2021. Conjointement à la mise en place d'un réseau de référents numériques, l'OSIIC a priorisé et mis en œuvre plusieurs chantiers de transformation, qui ont en retour nourri la feuille de route des solutions numériques qu'il propose au SGDSN. Qu'il s'agisse de mobilité, d'outils collaboratifs, ou encore de refonte de la relation client ou d'uniformisation de l'équipement numérique des salles de réunion, plusieurs de ces chantiers ont porté leurs premiers fruits en 2021. L'OSIIC a également apporté son concours au chantier parallèle de la transformation RH, en accompagnant la migration et la refonte des outils de gestion des ressources humaines.

Quelles ont été les conséquences de la dématérialisation des échanges et de la mobilité ?

Les systèmes d'information interministériels conçus et exploités par l'OSIIC au profit des très hautes autorités et de l'interministériel ont été plus que jamais sollicités, pour permettre la poursuite des activités les plus régaliennes de l'État dans un contexte de dématérialisation imposée des échanges. Les solutions de téléphonie et de vidéoconférence classifiées OSIRIS et HORUS ont ainsi servi de support régulier au conseil des ministres.

Le déploiement à large échelle de ces solutions a constitué une priorité pour l'OSIIC. Grâce à des gains d'efficacité, le nombre de terminaux déployés a pu être doublé en une année, tout en développant une couverture de l'ensemble du territoire national (notamment à travers le réseau des préfectures, presque toutes équipées au cours de l'année), et en initiant un déploiement au profit de nos emprises diplomatiques.

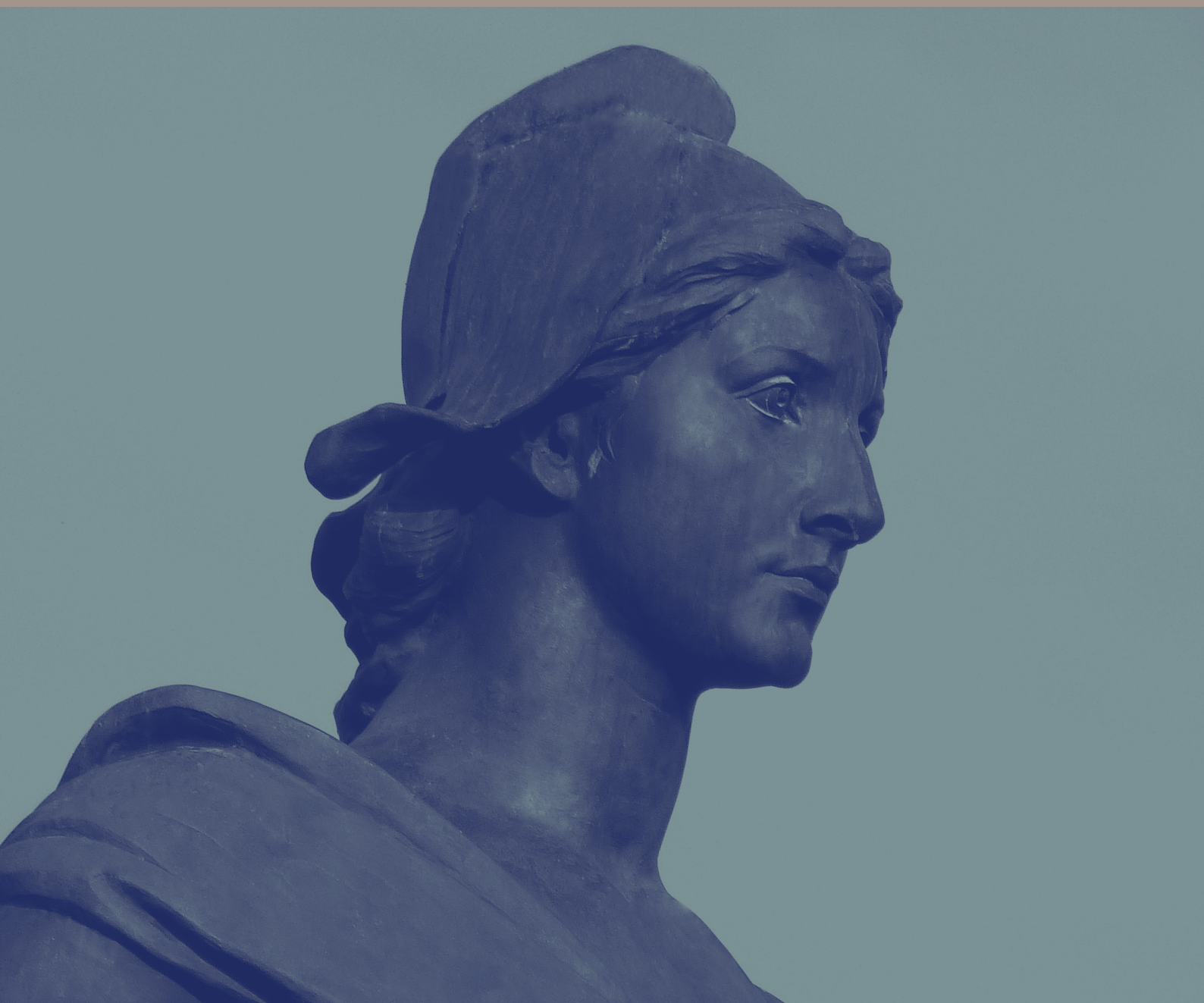
Cette couverture améliorée s'est doublée d'une convergence technologique entre les solutions spécifiques proposées au Président de la République et au Premier ministre d'une part, et les moyens fournis aux ministères et à leurs administrations d'autre part. Outre des échanges sécurisés « sans couture » entre l'ensemble des autorités et services de l'exécutif, ces évolutions ont permis quelques prouesses technologiques : un premier conseil des ministres intercontinental, en juillet, réunissant le Gouvernement rassemblé à Paris et le Président de la République en vol au-dessus de l'Océan Pacifique, de retour d'un déplacement en Polynésie Française, mais aussi plusieurs conseils des ministres ou de défense et de sécurité nationale en réponse à l'urgence sanitaire, pendant la période estivale ou celle de fin d'année, rassemblant des ministres répartis dans le réseau des préfectures sur l'ensemble du territoire national.

Où en est-on du chantier Néo 2 ?

La solution de *smartphone* sécurisée Secdroid, dont le développement a été transféré à l'OSIIC à sa création, est intégrée depuis 2014 dans les terminaux mobiles Néo des forces de sécurité intérieures. La notification par le ministère de l'intérieur du marché Néo 2, pour la rénovation de ces terminaux, a initié en 2021 une nouvelle coopération très intense entre l'OSIIC et le service des technologies et des systèmes d'information de la sécurité intérieure – ST(SI)^2 – afin d'intégrer une nouvelle version de Secdroid sur ces terminaux, désormais fournis par la société française Crosscall. Les travaux d'intégration logicielle ont ainsi débuté au cours de l'été, avec un calendrier ambitieux prévoyant une première livraison en mars 2022, puis le déploiement de 200 000 terminaux en six mois.

Cette coopération devrait permettre une avancée majeure dans l'outillage numérique des forces de sécurité intérieure, sur la base d'une solution sécurisée, souveraine, et maîtrisée d'un point de vue budgétaire. Elle apportera également des améliorations importantes à la solution Secdroid, dont bénéficieront ses autres utilisations par l'OSIIC, et une maîtrise accrue par l'opérateur des technologies clés de mobilité sécurisée.

Détecter et caractériser



Les ingérences numériques étrangères : une menace récente et durable à prendre au sérieux

Intégrée dans des stratégies dites hybrides, l'ingérence numérique étrangère est un levier de compétition ou de confrontation à l'échelle internationale. Elle est couramment utilisée par des États ayant la volonté de projeter leur puissance hors de leurs frontières. La menace émane également de certains mouvements non-étatiques, structurés ou non. Elle passe par l'instrumentalisation des plateformes numériques.

En France, l'assassinat de M. Samuel Paty, le 16 octobre 2020, a illustré la dualité du rôle des plateformes numériques. Les réseaux « sociaux » ont joué un rôle déterminant dans la propagation des rumeurs qui ont abouti au drame. Ils ont aussi largement relayé l'expression de la solidarité avec la victime et le rejet des extrémismes. Toutefois, une fois l'évènement passé, la France a fait l'objet de mises en cause publiques de la part de certains États. Elle était notamment accusée de discriminer une partie de la population en raison de ses convictions religieuses. Insidieusement, de nombreuses prises de positions antifrançaises sur les plateformes numériques ont attiré l'attention. Le SGDSN a alors été chargé de déterminer s'il s'agissait de prises de position individuelles et inauthentiques ou s'il s'agissait au contraire de manipulations. À cette fin, un groupe de travail nommé « Honfleur » a été constitué, rassemblant des experts du SGDSN et des ministères de la défense, de l'intérieur et du ministère de l'Europe et des affaires étrangères. À l'issue de plusieurs mois de recherche, le groupe de travail a conclu qu'une part importante des expressions hostiles à la France examinées étaient suscitées par une puissance étrangère, activant divers dispositifs artificiels et visant à influencer les internautes.

À l'issue de ces recherches, la décision a été prise de doter notre pays d'une structure en charge de lutter contre ce type de menace. Suite à un long processus de consultation qui s'est étalé durant le premier semestre 2021, le service de vigilance et de protection contre les ingérences numériques étrangères a été créé le 13 juillet avec pour objectifs de mieux appréhender et détecter ces phénomènes, afin de s'en prémunir efficacement.

Chiffres clés
(au 31/12/2021)

2/3
d'agents contractuels

65
agents travailleront pour VIGINUM fin 2022

20
opérations de vigilance anticipées par an

La création de VIGINUM

VIGINUM est le service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères. Ses principales missions sont de détecter et de caractériser les phénomènes répondant aux quatre critères de définition d'une ingérence numérique étrangère :

- l'intention de porter atteinte aux intérêts fondamentaux de la Nation ;
- la propagation de contenus manifestement inexacts ou trompeurs ;
- la diffusion inauthentique (artificielle ou automatisée, massive et délibérée) destinée à amplifier la visibilité ou la viralité de ces contenus ;
- l'implication, directe ou indirecte, d'un acteur étranger, étatique ou non.

VIGINUM emploie des spécialistes sélectionnés pour leur expertise en recherche et analyse numériques en source ouverte, en science de la donnée, en algorithmie, en investigation, en science politique et géopolitique. Mêlant des profils issus de la sphère régalienne et du domaine du numérique, ce collectif est la rencontre de deux mondes.

Ce nouveau service travaille en lien étroit avec l'ensemble des administrations contribuant à la lutte contre la manipulation de l'information : armées, diplomatie, directions du ministère de l'intérieur, etc. Le service entretient également des relations suivies avec les acteurs clefs que sont les plateformes numériques, la sphère industrielle, le monde de la recherche, des partenaires internationaux ainsi que des autorités indépendantes telles que l'ARCOM et la CNIL.

Les opérations de vigilance et de protection

L'activité de VIGINUM est tournée vers la conduite d'opérations. Chacune d'entre elles couvre une composante du débat public touchant aux intérêts fondamentaux de la Nation. Elle assure une posture de vigilance face à une menace informationnelle potentielle. Concrètement, il peut s'agir d'événements institutionnels, politiques, sociétaux, sportifs, planifiés ou imprévus, en lien avec l'actualité ou non, se déroulant en France ou ayant une incidence dans le débat national. Par exemple, les principaux scrutins nationaux donnent lieu à l'ouverture d'une opération.

Chaque opération est menée par une équipe d'experts, animée par un chef de projet. Cette équipe est spécifiquement constituée pour répondre à la menace, à son contexte, à ses enjeux, ainsi qu'à son intensité.

Un cadre juridique et éthique rigoureux

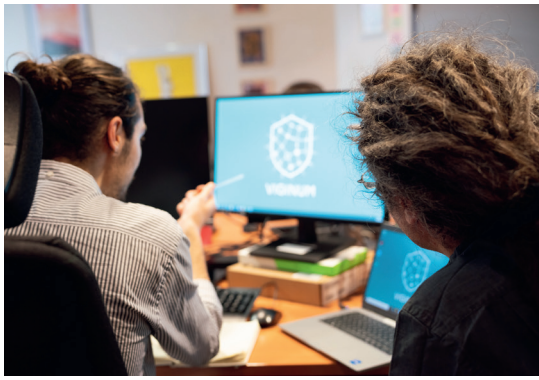
L'activité opérationnelle de VIGINUM s'inscrit dans un cadre juridique et éthique rigoureux.

Le décret n° 2021-1587 du 7 décembre 2021, pris après avis de la Commission nationale de l'information et des libertés (CNIL), définit les conditions dans lesquelles le service est autorisé, pour l'exercice de ses missions, à recueillir des données à caractère personnel : plateformes concernées, types de données recueillies, méthode de sélection, durée du recueil, conditions de renouvellement, obligation de suppression des données, sécurité du dispositif, exercice des droits d'accès de rectification et de suppression, etc. Les modalités de recueil de données à caractère personnel par le service sont contrôlées par la CNIL.

Par ailleurs, un comité éthique et scientifique présidé par M^me^ Béatrice Bourgeois-Machureau, conseillère d'État, a été placé le 15 octobre 2021 auprès du secrétaire général de la défense et de la sécurité nationale. Sa mission est de suivre l'activité de VIGINUM et de produire un rapport public. ◄

Une opération pour sécuriser l'élection présidentielle

Dès novembre 2021, VIGINUM a lancé une opération destinée à détecter et à caractériser d'éventuelles campagnes d'ingérences numériques étrangères visant l'élection présidentielle de 2022. Pour cette opération, conformément au cadre réglementaire, VIGINUM a été mis au service des garants du bon déroulement de l'élection : la Commission nationale de contrôle de la campagne électorale (CNCCEP), l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) ainsi que le Conseil constitutionnel. ◄



VIGINUM a pour mission de détecter et caractériser tout phénomène d'ingérence étrangère sur les plateformes numériques.

Questions à...

Gabriel Ferriol

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

Dix mois après sa création, où en est l'installation de VIGINUM ?

Beaucoup de choses ont été accomplies depuis le lancement de la mission de préfiguration au printemps 2021. L'encadrement juridique du service a tout d'abord été défini avec la publication de deux décrets. Le premier, en date du 13 juillet 2021, a créé VIGINUM et a défini ses missions. Le second, publié le 7 décembre 2021, autorise et encadre le recours par le service à un traitement de données à caractère personnel. Notre collectif de travail s'est en parallèle étoffé. Plus d'une trentaine de spécialistes l'ont rejoint. Nous avons pour objectif de poursuivre cette montée en puissance et de doubler nos effectifs à la fin de l'année 2022. Nous nous équipons par ailleurs d'outils d'analyse, en particulier d'une infrastructure informatique qui nous soit propre, de manière à être autonomes dans la réalisation de nos missions. Enfin, nous développons la coopération avec nos partenaires, notamment à l'échelle interministérielle où nous animons et coordonnons un réseau technique rassemblant les administrations contribuant à la lutte contre les manipulations de l'information, sous l'autorité du SGDSN.

Comment VIGINUM fait-il pour détecter les campagnes de manipulation de l'information ?

À l'ouverture d'une opération, le service établit le cadre de référence de ses travaux. Il observe le débat public, dresse un état de la menace, s'attache à identifier les plateformes intéressantes ainsi que les éventuels acteurs d'intérêt qui y sont actifs. Nous déterminons également des listes de critères techniques, notamment des mots-clés, pour approcher au mieux la thématique de l'opération. Une fois ce cadrage réalisé, l'opération entre dans sa phase active pendant laquelle VIGINUM va conduire en parallèle deux activités : l'une de détection, l'autre de caractérisation.

L'activité de détection consiste à identifier des marqueurs d'inauthenticité dans le débat numérique. Ces marqueurs peuvent concerner des comptes atypiques, des contenus suspects ou encore des comportements aberrants, anormaux ou coordonnés. En d'autres termes, l'activité de détection de VIGINUM consiste à mettre en évidence des « anomalies » affectant le déroulement du débat. Pour ce faire, nous utilisons notamment des métriques mathématiques conçues par les *datascientists* de notre Datalab.

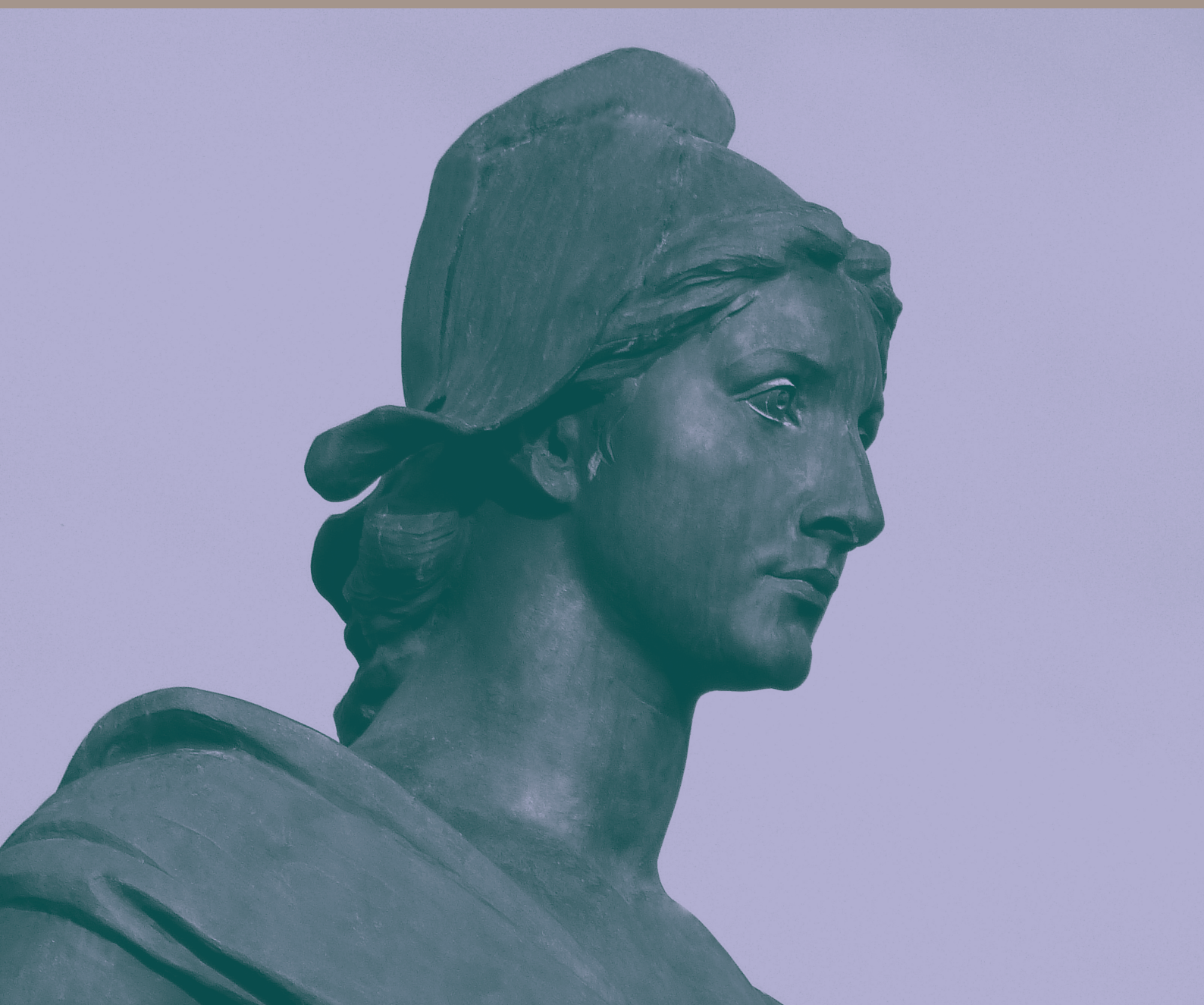
L'activité de caractérisation consiste, sur la base des éléments détectés, à vérifier si les phénomènes observés répondent ou non aux quatre critères de définition d'une ingérence numérique étrangère : intention de porter atteinte aux intérêts fondamentaux de la Nation, contenu manifestement inexact ou trompeur, amplification de la diffusion et implication, directe ou indirecte, d'un acteur étranger. Cette activité débouche sur la rédaction d'une ou de plusieurs note(s) d'analyse.

À la clôture de l'opération, le service supprime toutes les données à caractère personnel qu'il détiendrait encore, établit une synthèse de ses observations et opère un retour d'expérience destiné à tirer des enseignements de ses travaux.

Dans le cadre de ses missions, VIGINUM coopère-t-il avec d'autres organisations ?

La coopération avec les acteurs publics et privés est indispensable pour lutter efficacement contre la menace informationnelle. Nous animons le réseau technique réunissant les acteurs interministériels disposant de capacités de lutte contre la manipulation de l'information. Alors que VIGINUM travaille exclusivement sur des données publiquement accessibles (sources ouvertes), d'autres services de l'État disposent de leviers complémentaires pour enrichir l'analyse des phénomènes à risque. Nous nous inscrivons également dans une logique de collaboration avec le monde académique dont le rôle est essentiel pour forger les concepts, appréhender les phénomènes ou encore former les experts. Enfin, le service développe des coopérations, notamment avec les principales plateformes numériques qui ont accueilli favorablement sa création.

Soutenir et appuyer



Le GIC offre aux services de renseignement des outils d'exploitation des communications électroniques qu'il a collectées : contenus et métadonnées.

Une activité soutenue

L'activité opérationnelle du groupement interministériel de contrôle (GIC) s'est une nouvelle fois accrue en 2021. Elle a augmenté de 10 %. Chaque jour, le GIC a traité 350 demandes, a exercé son pouvoir de réquisition auprès des opérateurs ou fournisseurs de communications électroniques des milliers de fois et a validé 1100 transcriptions. Dans ce sens, le GIC a notamment étendu l'exercice de ses réquisitions auprès de nouveaux interlocuteurs, tels que des hébergeurs, des opérateurs de communications par satellite et des opérateurs ultra-marins. Il a ouvert un nouveau centre d'exploitation des interceptions de sécurité et a entièrement déménagé et modernisé un centre d'exploitation, sans interruption d'activité.

Par ailleurs, les évolutions du cadre légal et règlementaire ont eu des impacts importants sur l'activité du GIC. Les systèmes d'information ont été adaptés aux modifications induites par la nouvelle version de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale. De même, les modifications induites par le nouveau décret relatif aux services du second cercle ont été prises en compte. D'autre part, le GIC a largement contribué à l'élaboration du projet de loi PATR[1] au cours du premier semestre, puis à la mise en œuvre de la loi dès son entrée en vigueur.

En matière de lutte contre le terrorisme, le GIC a poursuivi la mise en œuvre des traitements automatisés autorisés en application de l'article L. 851-3 du code de la sécurité intérieure. Il a lancé en octobre les travaux pour étendre ces traitements aux données internet, au terme d'un cadrage entamé dès l'été 2020.

Dans le domaine du renseignement, plusieurs coopérations techniques ont été conduites avec les services, notamment sur l'affaire NSO Pegasus et sur le traitement automatique du langage.

En parallèle de ses activités opérationnelles et techniques, le GIC a adressé sept mémoires à la formation spécialisée du Conseil d'État chargé des contentieux en matière de techniques de renseignement, qui a rendu en 2021 sept décisions favorables au Premier ministre.

Dans le champ opérationnel, le GIC a constaté l'adoption de son dispositif centralisé de captation d'images par plusieurs services. Le groupement interministériel de contrôle a également pu déployer un outil spécifique d'exploitation hors de ses centres pour faciliter l'accès des services exploitants et il a accompagné chacun d'entre eux pour une bonne prise en main du dispositif centralisé. En 2021, 541 transcriptions de captations de paroles centralisées ont été validées, contre 122 en 2020. Enfin, l'exploitation centralisée au GIC des données de connexion qu'il recueille en temps réel est désormais possible.

Le GIC a consacré son activité technique aux évolutions des systèmes d'information qu'il développe et qu'il administre au profit des autorités et de la communauté du renseignement. De nombreuses modifications ergonomiques ont été apportées à l'outil de traitement des demandes. De surcroît, cet outil est désormais plus flexible dans sa capacité à prendre en compte des modifications des demandes. D'autre part, le traitement des demandes de recueil de données de connexion en temps réel est désormais dématérialisé. L'outil d'exploitation des interceptions de sécurité a évolué à plusieurs reprises dans le sens d'une meilleure ergonomie. L'outil d'exploitation des données de connexion a été perfectionné. Enfin, un service exploitant bénéficie d'une nouvelle liaison permettant le recueil dématérialisé du renseignement.

1. Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

Les moyens du GIC

Au cours de l'année, le GIC a poursuivi les évolutions et la sécurisation de son système informatique interne pour faciliter le travail à distance, rendu nécessaire par l'exiguïté des locaux et la crise sanitaire (améliorations des postes nomades déjà déployés et, avec l'OSIIC, déploiement de la téléphonie interministérielle sécurisée et de la visioconférence sécurisée). Pour son fonctionnement courant, le GIC a poursuivi les évolutions de son portail interne, a déployé un outil ergonomique de gestion des habilitations et des documents classifiés, un outil de travail collaboratif et un outil de gestion de portefeuille de projet.

Alors qu'il a connu des mouvements de personnels importants en 2021 (24 %) et procédé à près d'une cinquantaine de recrutements, l'atteinte de la cible des effectifs demeure une préoccupation permanente pour assurer la plénitude des missions. Les compétences recherchées relèvent principalement du domaine de l'informatique, des réseaux, des télécoms et de la cybersécurité. Fait rare au sein de l'État, le GIC dispose d'équipes de développeurs au plus près du noyau Linux, des *développeurs back*, *front* ou *fullstack* d'applications métiers sur des technologies *cloud-native* (kubernetes, bus *kafka*, microservices, authentification SSO), ainsi que des data *engineers* et des data *scientists* compétents en technologies *Big Data* (Hadoop, Elastic Search…). De plus, l'ensemble de l'informatique du GIC nécessite des équipes d'administrateurs des systèmes et réseaux particulièrement compétents en matière de cybersécurité. Pour tous ces métiers en tension, le recrutement de nouveau agents et leur fidélisation constituent la priorité du GIC en 2022.

Sur le plan financier, le GIC a exécuté son budget 2021 à 98 % et, en suivant les recommandations de la commission de vérification des fonds spéciaux, a poursuivi la bascule sur fonds budgétaires de droit commun de dépenses autrefois effectuées en fonds spéciaux. Il a restitué des fonds spéciaux au dernier trimestre. ◄

Chiffres clés
(au 31/12/2021)

Un système d'information déployé sur près de

70
sites

2000
postes de travail déployés

6000
comptes informatiques actifs

413
formations dispensées aux agents des services exploitants sur l'utilisation des applications du GIC

Une croissance de l'activité de

10 %
en un an

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