
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN
SECRÉTARIAT GÉNÉRAL
DE LA DÉFENSE
ET DE LA SÉCURITÉ NATIONALE
RAPPORT
D'ACTIVITÉ
2015

Édité par le secrétariat général de la défense et de la sécurité nationale (SGDSN)
Directeur de la publication : Louis Gautier
Coordination : Gwénaël Jézéquel
Conception et réalisation : PCA / Vincent Treppoz
Crédits photos : Sébastien ORTOLA, Jean Claude MOSCHETTI, Juliette ROBERT, HAMILTON, LUDOVIC, Gilles ROLLE, Ian HANNING, Nicolas TAVERNIER (Agence Réa) - Istock - WikiCommons - DR
Impression : Direction de l'information légale et administrative (DILA)
Juillet 2016

SOMMAIRE

Les problèmes de sécurité ne peuvent plus être traités comme auparavant

Louis Gautier, secrétaire général de la défense et de la sécurité nationale, revient sur les missions du SGDSN et sur les principaux enseignements d'une année 2015 dramatique.

QUE PEUT-ON DIRE DES MISSIONS ET DE LA PLACE DU SGDSN ?

Placé sous l'autorité du Premier ministre, le SGDSN joue un rôle essentiel dans l'instruction et le suivi des décisions de l'exécutif intéressant la défense et la sécurité nationale. Il assure le secrétariat des conseils de défense et de sécurité nationale que préside le chef de l'État. Il coordonne l'action des ministères dans les domaines de la sécurité et de la défense. Il exerce en propre et par délégation du Premier ministre de nombreuses fonctions interministérielles. À ce titre, lui sont rattachés divers organismes comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le centre de transmissions gouvernemental (CTG) ou encore l'Institut des hautes études de défense nationale (IHEDN) et l'Institut national des hautes études de la sécurité et de la justice (INHESJ). Ainsi le SGDSN n'agit-il pas seulement comme « secrétariat général » ayant, dans son domaine de compétences, un rôle d'animateur et de coordonnateur de l'action interministérielle. Il est également, lui-même, opérateur de sécurité.

S'IL FALLAIT RÉSUMER, QUELS SONT LES QUALIFICATIFS OU LES VALEURS QUI CARACTÉRISENT LE MIEUX LE SGDSN ?

La cohérence et la continuité de l'action de l'État dans le domaine de la défense et de la sécurité. À cette fin, le SGDSN, qui se trouve à la confluence des diverses sources publiques d'information et du renseignement, doit être une vigie pour détecter toutes les menaces pouvant affecter notre pays. Dans une logique de prévention, il doit également planifier en amont les réponses de l'administration comme dans le plan Vigipirate qu'il actualise et met en œuvre. Il lui appartient enfin d'assurer, dans la gestion des crises, la préparation et le suivi des décisions de l'exécutif. Pour l'ensemble de ces missions, le SGDSN peut s'appuyer sur des agents de cultures professionnelles très variées – militaires, membres du corps préfectoral, diplomates, ingénieurs civils et militaires… –, mais aussi sur des experts scientifiques de haut niveau. Ce vivier est à la fois sa particularité et sa richesse.

QUELS ONT ÉTÉ, POUR VOUS, LES FAITS MARQUANTS DE 2015 ?

L'année 2015 a été dramatique. Les attentats de janvier et de novembre figurent bien sûr au premier plan. Il a fallu apporter des réponses d'application immédiate sur le territoire national, notamment en renforçant tous nos dispositifs de prévention et de protection, tout en veillant à la bonne exécution des opérations militaires menées par la France contre Daech ou Al-Qaïda, que ce soit en Irak, en Syrie ou au Sahel. Le SGDSN a pris toute sa part dans l'élaboration de ces politiques. C'est notamment à ce titre qu'il a assuré le suivi d'une douzaine de conseils de défense et de sécurité nationale. Pour autant, le SGDSN est resté très actif sur bien d'autres chantiers, comme la loi relative au renseignement du 24 juillet 2015, dont il a été l'un des artisans, la rédaction de la stratégie nationale de cybersécurité ou le rapport sur l'essor des drones civils en France.

CONSEILLER-MAÎTRE À LA COUR DES COMPTES, LOUIS GAUTIER EST LE SECRÉTAIRE GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE DEPUIS OCTOBRE 2014. AUPARAVANT, IL A NOTAMMENT ÉTÉ CONSEILLER POUR LA DÉFENSE DU PREMIER MINISTRE, CONSEILLER, PUIS DIRECTEUR ADJOINT DU CABINET DU MINISTRE DE LA DÉFENSE ET CONSEILLER AU CABINET DU MINISTRE DE L'INTÉRIEUR.

Le SGDSN a également été associé à de grands dossiers industriels. Il a notamment négocié le protocole d'accord intergouvernemental franco-allemand, à l'occasion de la fusion de Nexter-KMW. Du côté de l'ANSSI, il y a eu le traitement de la cyberattaque contre TV5 Monde. Enfin, le SGDSN a poursuivi sa croissance avec l'augmentation des effectifs de l'ANSSI et le rattachement du GIC.

IL Y A EU AUSSI LA NÉGOCIATION SUR LES BPC MISTRAL…

Ce fut un dossier extrêmement sensible. Le mandat des négociations fut confié par l'Élysée au SGDSN en raison de sa capacité à faire travailler ensemble plusieurs départements ministériels directement concernés par cette question. Il fallait à la fois analyser les enjeux de la négociation diplomatique avec les Russes – acceptation d'une solution amiable, montant des indemnités à prévoir… –, mais aussi prendre en considération des aspects plus nationaux liés aux risques de retombées industrielles – destructions d'emplois, faillites éventuelles, dédommagement de la Coface… Notre positionnement nous a permis de faire prendre conscience de ces enjeux à l'ensemble des parties prenantes en France, dont DCNS, et de négocier au mieux de nos intérêts avec la partie russe. Cela a permis un débouclage rapide du dossier et une économie substantielle par rapport à un contentieux autrement inéluctable. Cet épisode a confirmé la pleine capacité opérationnelle du SGDSN.

POURQUOI UNE TELLE CONCENTRATION DE CONSEILS DE DÉFENSE EN 2015 ET QUEL A ÉTÉ LE RÔLE DU SGDSN ?

Le contexte que j'évoquais tout à l'heure y est évidemment pour beaucoup. L'intérêt de ces conseils est de réunir autour du Président de la République tous les principaux responsables politiques et administratifs intéressés par le sujet traité. Le SGDSN, qui y occupe une place permanente, veille à la cohérence du processus, de la préparation du conseil à l'ampliation des décisions.

QUELLES SONT LES PERSPECTIVES D'ÉVOLUTION DU SGDSN À COURT ET MOYEN TERME ?

La première priorité reste la lutte contre le terrorisme et ses nouvelles formes, qui suppose des coopérations internationales accrues que le SGDSN entend favoriser. Le SGDSN doit également contribuer, sur le plan national, à la consolidation des industries de sécurité, à travers le CoFIS, le comité de la filière industrielle de sécurité. Sur le plan institutionnel, il doit veiller au développement de l'ANSSI et, notamment, à la régionalisation de son organisation, et conduire à bon port la réforme du groupement interministériel de contrôle (GIC), qui vient de lui être organiquement rattaché.

Le SGDSN en quelques mots

En 2009, conformément aux orientations du Livre blanc sur la défense et la sécurité nationale et aux dispositions de la loi relative à la programmation militaire pour la période 2009-2014, le secrétariat général de la défense nationale (SGDN) s'est transformé en un secrétariat général de la défense et de la sécurité nationale (SGDSN), doté de missions élargies.

Placé sous l'autorité du Premier ministre, le SGDSN assiste le chef du Gouvernement dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Il agit ainsi en appui de la prise de décision politique. Son champ d'intervention couvre l'ensemble des questions stratégiques de défense et de sécurité, dans le domaine de la programmation militaire, de la politique de dissuasion, de la sécurité intérieure concourant à la sécurité nationale, de la sécurité économique et énergétique, de la lutte contre le terrorisme et de la planification des réponses aux crises.

Le SGDSN en quelques chiffres

160 M€
DE BUDGET EN 2015.

896
AGENTS.

49
JOURNÉES DE PARTICIPATION À LA CELLULE INTERMINISTÉRIELLE DE CRISE.

26
MODIFICATIONS DE LA POSTURE VIGIPIRATE.

80 %
DES AGENTS DE L'ANSSI SONT INGÉNIEURS ET/OU DOCTEURS EN INFORMATIQUE, CRYPTOLOGIE, MATHÉMATIQUES, ÉLECTRONIQUE, PHYSIQUE…

8 240
DEMANDES D'EXPORTATION DE MATÉRIELS DE GUERRE ET DE BIENS À DOUBLE USAGE EXAMINÉES EN 2015.

Le SGDSN assure trois missions principales. La première porte sur la veille et l'alerte face aux menaces et aux risques. Dans ce cadre, il est chargé du suivi des crises, de la préparation des plans gouvernementaux et de l'organisation de l'État en temps de crise. Deuxième fonction : le conseil et la rédaction des décisions prises par l'exécutif en matière de défense et de sécurité nationale. Le SGDSN contribue ainsi à l'élaboration des projets de loi et des textes réglementaires dans ses domaines de compétences.

Enfin, le SGDSN agit comme opérateur, notamment dans la gestion des habilitations, des documents classifiés, des communications gouvernementales – à travers la gestion du centre de transmissions gouvernemental (CTG) – ou encore de la sécurité des systèmes d'information et la cyberdéfense. Rattachée au SGDSN, c'est l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui assure cette dernière mission. Par ailleurs, le SGDSN exerce la tutelle de l'Institut des hautes études de défense nationale (IHEDN) et de l'Institut national des hautes études de la sécurité et de la justice (INHESJ).

230
SITES RACCORDÉS AU RÉSEAU DE DONNÉES INTERMINISTÉRIEL « CONFIDENTIEL DÉFENSE » (ISIS).

40
PUBLICATIONS DE RECHERCHE SUR DES SUJETS AUSSI VARIÉS QUE LA CRYPTOGRAPHIE OU LA RECONNAISSANCE VOCALE.

24h/24
ET 7 JOURS SUR 7, LE BUREAU « VEILLE ET ALERTE » INFORME LES AUTORITÉS DES ÉVÈNEMENTS GRAVES ET IMPRÉVUS.
LE CTG VEILLE AU BON FONCTIONNEMENT DES RÉSEAUX PROTÉGÉS.

4 000
SIGNALEMENTS REÇUS D'ATTAQUES INFORMATIQUES, SOIT 50 % DE PLUS QU'EN 2014.

3
PROJETS COFINANCÉS AU TITRE DE LA LUTTE ANTIDRONES.

7
ACCORDS INTERNATIONAUX DE SÉCURITÉ, EN COURS DE NÉGOCIATION EN 2015, QUI S'AJOUTERONT AUX 35 DÉJÀ SIGNÉS PAR LA FRANCE.

Le SGDSN en 2015

7, 8 et 9 janvier

ATTAQUES TERRORISTES À PARIS ET MONTROUGE.

26 février

DÉBUT DES NÉGOCIATIONS AVEC LA RUSSIE SUR LE CONTRAT DES BPC MISTRAL.

24 mars

PUBLICATION DU *GUIDE DES BONNES PRATIQUES DE L'INFORMATIQUE*, ÉDITÉ PAR L'ANSSI.

27 mars

SIGNATURE DE TROIS DÉCRETS RELATIFS À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.

8 avril

ATTAQUE INFORMATIQUE DE TV5 MONDE ET INTERVENTION DE L'ANSSI.

21 mai

DÉPLOIEMENT, POUR CINQ MOIS, DU CENTRE DE TRANSMISSIONS GOUVERNEMENTAL SUR SON SITE DE SECOURS, PENDANT LES TRAVAUX DE MODERNISATION DU SITE PRINCIPAL.

28 mai

ORGANISATION DU COLLOQUE INTERNATIONAL SUR LES DRONES CIVILS ET LA SÉCURITÉ.

30 septembre

PARTICIPATION DE L'ANSSI AUX 15E ASSISES DE LA SÉCURITÉ À MONACO.

6 et 7 octobre

EXERCICE GOUVERNEMENTAL DE SIMULATION EUROFOOT 15, DESTINÉ À PRÉPARER L'EURO 2016 DE FOOTBALL.

16 octobre

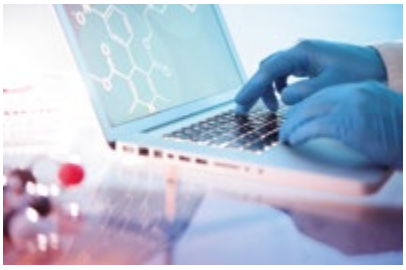
PRÉSENTATION DE LA STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE, COORDONNÉE PAR L'ANSSI.

20 octobre

REMISE AU GOUVERNEMENT DU RAPPORT SUR L'ESSOR DES DRONES CIVILS EN FRANCE.

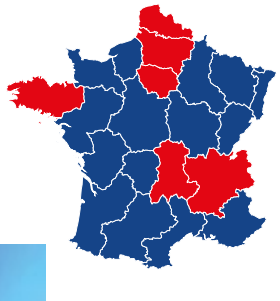
13 novembre

ATTAQUES TERRORISTES À PARIS (10E ET 11E ARRONDISSEMENTS) ET À SAINT-DENIS (STADE DE FRANCE).



15 novembre

INSTALLATION DU CONSEIL NATIONAL CONSULTATIF POUR LA BIOSÉCURITÉ (CNCB).



4 décembre

DÉBUT DU DÉPLOIEMENT DES RÉFÉRENTS DE L'ANSSI EN RÉGION (ÎLE-DE-FRANCE, HAUTS-DE-FRANCE, BRETAGNE ET AUVERGNE-RHÔNE-ALPES).

15 décembre

REMISE AU PREMIER MINISTRE DU RAPPORT SUR LA GESTION DES ATTENTATS DE PARIS.

17 décembre

PUBLICATION DU RAPPORT SUR LE SECRET DE LA DÉFENSE NATIONALE EN FRANCE 2015.

29 décembre

REMISE DU RAPPORT DE RÉÉVALUATION DU PLAN VIGIPIRATE.

Temps forts

CYBERATTAQUE : L'ANSSI AU CHEVET DE TV5 MONDE

Mercredi 8 avril 2015, vers 21 heures. L'attaque informatique contre TV5 Monde commence. En très peu de temps, des pirates mettent la chaîne hors d'état de diffuser ses programmes. Par la suite, une revendication de Daech est diffusée. Les comptes Twitter, la page Facebook et la page d'accueil du site internet de TV5 Monde sont également défigurés, tandis que la messagerie et le système d'information de la chaîne sont hors d'usage. Une attaque d'envergure menée à des fins de sabotage – une première en France –, portée immédiatement à la connaissance de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Bien que TV5 Monde ne fasse pas partie de son périmètre d'action – les administrations et les opérateurs d'importance vitale (OIV), principalement –, l'agence intervient rapidement. Jusqu'à vingt agents sont dépêchés dans les locaux de la chaîne pour reconstruire et sécuriser le système d'information endommagé, en collaboration avec les équipes de TV5 Monde. Au terme de cette intervention éclair, la diffusion reprend progressivement dès le lendemain. Cependant, la mission de l'ANSSI s'est poursuivie jusqu'en juillet et s'est conclue par une prise de relais par des prestataires privés de confiance, spécialisés en cybersécurité.

LE DÉNOUEMENT DU DOSSIER DES BPC MISTRAL

Le 4 décembre 2014, le Premier ministre a confié au secrétaire général la mission d'envisager les conséquences, puis, en 2015, de négocier la non-livraison de deux bâtiments de projection et de commandement (BPC) à la Fédération de Russie. Il s'agissait de trouver une issue à la non-exécution des obligations du contrat industriel et de l'accord intergouvernemental liés à cette livraison. Pendant plusieurs mois, le SGDSN a coordonné et consolidé la position française, avec les ministères concernés et DCNS, le constructeur. Après des dizaines d'allers-retours entre Moscou et Paris, dans la plus grande confidentialité, l'accord a été soumis à l'arbitrage du Président de la République et du Premier ministre en août 2015, avant que sa ratification ne soit autorisée par le Parlement.

DES DRONES SOUS SURVEILLANCE

Après les survols non autorisés de drones au-dessus de sites sensibles, le Premier ministre a confié au SGDSN la mission d'animer une réflexion interministérielle sur le sujet et de présenter des propositions susceptibles de permettre une lutte plus efficace contre l'emploi de ces appareils à des fins malveillantes. Grâce à l'apport de nombreux contributeurs (direction générale de l'aviation civile, armée de l'air, forces de sécurité intérieure, opérateurs…), ce travail a abouti à la remise d'un rapport au chef du Gouvernement au mois d'octobre 2015. Le document présente un état des lieux de ce secteur d'activité en plein essor, ainsi qu'un inventaire des risques et des menaces associés à une utilisation détournée de ces aéronefs. Le rapport préconise également une série de mesures destinées à mieux encadrer cette activité, tout en veillant à ne pas freiner son développement. Il explore aussi des solutions techniques de détection, d'identification et de neutralisation de ces aéronefs de petite taille. Dans ce domaine, le SGDSN a lancé, fin 2014, un appel à projets, par le biais de l'Agence nationale de la recherche (ANR). Objectif : à partir des technologies les plus innovantes, proposer dans un délai de 12 à 18 mois des démonstrateurs capables de détecter, d'identifier et de neutraliser des drones aériens civils de petites dimensions.

VIGIPIRATE : UNE ADAPTATION PERMANENTE À LA MENACE

Le plan gouvernemental Vigipirate répond à une triple exigence : vigilance, prévention et protection. Il couvre l'ensemble des activités du pays et participe à la sécurité nationale. Il s'agit d'un dispositif permanent, qui associe tous les acteurs de la Nation : l'État, les collectivités territoriales, les opérateurs d'importance vitale et les citoyens. Afin de répondre à l'évolution de la menace et des risques, le plan est régulièrement actualisé. Le contexte dramatique de l'année 2015, marqué par la vague d'attentats terroristes sur le territoire, s'est traduit par des adaptations successives. Elles consistent en des améliorations à apporter au dispositif de pilotage et aux procédures de mise en œuvre du plan. Elles portent également sur l'adaptation des niveaux de postures au niveau de la menace. Ainsi, en 2015, le SGDSN a diffusé – sur décision du cabinet du Premier ministre – vingt-six postures Vigipirate. Ce nombre élevé – d'ordinaire, le SGDSN diffuse quatre à cinq postures par an – traduit l'activité particulièrement dense de la cellule « Vigipirate » du SGDSN, tout au long de cette année.

Coordo

nner

Piloter

Sous l'autorité du Premier ministre, le SGDSN remplit nombre de missions régaliennes en matière de sécurité et de réponse aux crises, notamment par le biais du secrétariat des conseils de défense et de sécurité nationale. Sa position interministérielle lui vaut également d'animer et de coordonner différents travaux dans ce domaine, mais aussi d'assurer un suivi des crises internationales, susceptibles d'affecter la sécurité du territoire.

Le secrétaire général de la défense et de la sécurité nationale assiste le Premier ministre, en liaison étroite avec la présidence de la République, dans les domaines de la défense et de la sécurité nationale. À ce titre, le secrétariat des conseils de défense et de sécurité nationale (CDSN) constitue la mission historique du SGDSN. Depuis plus d'un siècle, cette instance a connu des périmètres et des dénominations variés, conférant de ce fait un rôle plus ou moins important aux prédécesseurs du SGDSN. La situation a profondément évolué avec la loi de programmation militaire du 29 juillet 2009, qui a fondu les différents conseils traitant jusqu'alors de défense, de sécurité intérieure et de crises extérieures en une instance unique.

LE CDSN : UNE ENCEINTE STRATÉGIQUE

Présidé par le chef de l'État, en présence du Premier ministre, le conseil de défense et de sécurité nationale a compétence sur toutes les questions de défense et de sécurité : programmation militaire ou de sécurité intérieure, politique de dissuasion, sécurité économique et énergétique, lutte contre le terrorisme ou planification des réponses aux crises.

Outre sa configuration plénière, il comporte deux formations spécialisées, qui siègent dans une composition adaptée : le conseil national du renseignement et le conseil des armements nucléaires. Le premier définit les orientations et les priorités stratégiques, et planifie les moyens humains et techniques des services spécialisés de renseignement. Le second traite des différents aspects de la dissuasion nucléaire : doctrine, format des forces, programmes de simulation et d'armement, types d'armes… Le CDSN peut également se réunir en formation restreinte, en particulier pour évoquer les opérations extérieures.

Le code de la défense prévoit que le secrétaire général assure le secrétariat de ces conseils. À ce titre, il prépare les réunions du CDSN, dans une approche interministérielle, élabore les relevés de décision, notifie les décisions prises au cours de la réunion et suit leur mise en œuvre. S'agissant des conseils nationaux du renseignement, le SGDSN intervient en appui du coordonnateur.

En 2015, le CDSN s'est réuni à plus d'une dizaine de reprises dans ses différentes formations. Il a notamment traité de tous les grands événements ayant affecté ou ayant été susceptibles d'affecter la sécurité intérieure et extérieure de la France.

SGDSN ET RENSEIGNEMENT

Le SGDSN appuie les travaux du coordonnateur national du renseignement (CNR). Outre son rôle dans le conseil national du renseignement, il contribue aux évolutions du cadre juridique et apporte son soutien par l'organisation de groupes interministériels d'analyse et de synthèse. Il mène également, en lien avec le CNR et les ministères concernés, des actions de coopération internationale, en matière de prévention et de lutte contre le terrorisme, en particulier avec l'Allemagne, les États-Unis d'Amérique et le Royaume-Uni.

3 questions à

ÉVENCE RICHARD

ÉVENCE RICHARD, AUJOURD'HUI PRÉFET DE LA LOIRE, ÉTAIT EN 2015 DIRECTEUR DE LA PROTECTION ET DE LA SÉCURITÉ DE L'ÉTAT AU SGDSN.

Que retenez-vous de 2015 ?

Assurément, 2015 n'a pas été une année comme les autres. Le terrorisme bien sûr, mais aussi des accidents majeurs comme celui du vol Germanwings ou des crises sanitaires comme Ebola ont marqué l'année. Un seul chiffre : la cellule interministérielle de crise a été activée durant quarante-neuf jours, contre six à dix jours au cours d'une année ordinaire, correspondant le plus souvent à des exercices… Il y a eu aussi de nombreuses modifications du plan Vigipirate durant l'année. D'autres sujets nous ont également occupés, comme la question des drones, avec un travail qui a amené à la publication de deux arrêtés en décembre 2015.

Pourquoi le choix du SGDSN sur cette question sensible ?

Parce que c'est un sujet transversal, qui implique de nombreux acteurs. À partir de la lettre de mission du Premier ministre et après une analyse des enjeux, nous avons mis sur pied quatre groupes de travail thématiques interministériels. Le SGDSN les a animés et a ensuite proposé une synthèse et un ensemble de mesures au Premier ministre. Au-delà de cet exemple, la dimension de recherche et développement est très présente au sein des activités de la direction. C'est le cas, par exemple, avec le CoFIS, le comité de la filière industrielle de sécurité.

(…) la cellule interministérielle de crise a été activée durant quarante-neuf jours, contre six à dix jours au cours d'une année ordinaire.

Quelle est la part des exercices de sécurité dans votre activité ?

C'est un gros travail, mais il est indispensable. La préparation est essentielle avec, en particulier, le choix d'un scénario réaliste. Ensuite, il faut faire travailler tous les niveaux ministériels, en y adjoignant parfois des acteurs de terrain. On simule aussi la pression médiatique et on met des outils à la disposition des communicants, comme des plateaux télé fictifs ou des réactions sur les réseaux sociaux. Un autre point clé est le retour d'expérience, à chaud et à froid, dans les trois mois ; le tout débouchant sur des propositions d'ajustement des plans existants.

LA COORDINATION DES TRAVAUX INTERMINISTÉRIELS

Sous l'autorité du Premier ministre, le SGDSN est chargé de coordonner les travaux interministériels concourant à la stratégie de sécurité nationale, définie par le Livre blanc sur la défense et la sécurité nationale de 2008. Dans ce cadre, il anime différents travaux interministériels portant notamment sur :

- l'analyse des risques et des menaces ;
- l'organisation de l'État face aux crises majeures ;
- la planification gouvernementale ;
- l'identification des capacités de l'État, des collectivités territoriales et des opérateurs indispensables à la gestion des crises ;
- le développement des technologies de sécurité ;
- la continuité des transmissions gouvernementales ;
- la protection du secret de la défense nationale.

Le SGDSN a ainsi élaboré une nouvelle directive générale interministérielle, relative à la planification de défense et de sécurité nationale, signée par le Premier ministre le 11 juin 2015. Ce document remplace une directive remontant à 2001 et tient compte des évolutions du contexte. Il aborde l'ensemble des travaux de préparation des actions à conduire en situation de crise. Il tient davantage compte de la dimension européenne et internationale, intègre les effets de la nouvelle organisation des services de l'État et des collectivités territoriales, mais aussi la mise en place d'une nouvelle organisation gouvernementale de crise. Cette directive a été complétée par un document de procédure sur la conduite à tenir en cas d'événement grave, adressé au Premier ministre fin juillet 2015.

Les travaux de rénovation des plans gouvernementaux, menés en 2015, ont aussi porté sur le plan Vigipirate, dans le prolongement des attentats qui ont frappé la France. Le rapport correspondant a été remis au Premier ministre le 29 décembre 2015 (voir page 35). De même, cinq nouvelles directives nationales de sécurité (DNS) étaient en cours d'approbation en 2015. Elles portent sur le transport aérien, le transport maritime et fluvial, les transports terrestres, les activités judiciaires, ainsi que l'audiovisuel et l'information (voir page 34).

FINALISATION DU CONTRAT GÉNÉRAL INTERMINISTÉRIEL

L'année 2015 a également été marquée par l'élaboration du contrat général interministériel (CGI). Complétant les « contrats opérationnels » des armées, ce document, qui couvre la période 2015-2019, précise les capacités critiques des ministères et leur niveau d'engagement en cas de crises majeures. Ceux-ci peuvent en effet être les premiers à intervenir face à certains risques ou menaces. Le CGI se compose d'un tronc commun et de deux volets spécifiques, consacrés à la sécurité des systèmes d'information et à la réponse aux menaces nucléaires, radiologiques, biologiques et chimiques (NRBC).

FACE À L'URGENCE

Dans le même esprit, le SGDSN a également engagé, en 2015, une étude préalable à la mise sur pied d'un dispositif logistique interministériel, qui serait déclenché en cas de crise majeure, particulièrement urgente ou complexe. Ce dispositif devrait associer à la fois des moyens publics et des moyens privés. Les conclusions seront remises au Premier ministre dans le courant de l'année 2016.

ANTICIPATION DES CRISES INTERNATIONALES

À travers sa direction des affaires internationales, stratégiques et technologiques (AIST), le SGDSN assure – à la demande du cabinet du Premier ministre ou de la présidence de la République, ou de sa propre initiative – des fonctions de veille et d'alerte, d'analyse et de synthèse, ainsi que d'aide à la décision sur des questions de sécurité internationale, susceptibles d'affecter les intérêts de la France. Ce suivi porte notamment sur les conflits dans lesquels sont engagées les forces françaises.

Ce travail prend notamment la forme de « fiches pays », synthétisant la situation et les perspectives d'évolution d'une zone géographique. Élaborés dans une approche interministérielle et dans une optique d'anticipation et de prévention, ces documents ont porté sur six pays en 2014-2015. Quatre autres pays et thèmes sont au programme en 2015-2016.

LE PILOTAGE DES STRATÉGIES INTERMINISTÉRIELLES

Le SGDSN assure également le suivi de plusieurs questions de nature stratégique : terrorisme, défense anti-missile balistique (DAMB), sécurité transatlantique et européenne, désarmement et maîtrise des armements, lutte contre les menaces liées aux flux illicites, lutte contre la piraterie maritime…

Sur ces différents points, le SGDSN coordonne la réflexion interministérielle sur les évolutions susceptibles d'avoir un impact sur les intérêts de la France. Il propose au Président de la République et au Premier ministre des orientations permettant de renforcer la sécurité nationale sur ces questions. Dans ce cadre, il produit notamment une évaluation mensuelle de la menace terroriste.

En 2015, le SGDSN a aussi assuré une coordination interministérielle sur la question de la DAMB, dans la perspective du prochain sommet de l'Otan, prévu à Varsovie à l'été 2016.

De même, il coordonne, depuis 2013, les travaux du groupe de prévention et de lutte contre la dissémination des armements conventionnels. Il vise notamment à appuyer les pays africains francophones dans la mise en place des outils de contrôle de ces armements.

Enfin, depuis 2008, le SGDSN pilote la stratégie interministérielle sur la région sahélo-sahélienne. Il s'agit à la fois de contribuer à la stabilisation et à la sécurisation de cette région (aide à la gouvernance, soutien et formation des administrations et des forces de sécurité, aide au développement…) et d'articuler la stratégie française avec celles de l'ONU, de l'Union européenne et des grands pays partenaires.

LE NUCLÉAIRE AUSSI

En matière de sécurité des installations nucléaires, la loi du 2 juin 2015 relative au renforcement de la protection des installations civiles abritant des matières nucléaires a créé un délit d'intrusion, puni d'un an d'emprisonnement et de 15 000 euros d'amende. Les travaux sur le décret d'application sont en cours, ainsi que ceux sur les compétences des services de sécurité des opérateurs et leurs dispositifs de protection physique. L'année précédente, le SGDSN avait coordonné l'élaboration d'une convention d'assistance entre l'État et EDF pour la projection, par voie aérienne, d'une équipe de reconnaissance de la force d'action rapide nucléaire (Farn) de l'opérateur, en cas de situation d'urgence sur une installation.

MIEUX EXPLOITER LA PROSPECTIVE

L'exploitation des différentes synthèses sur l'évolution internationale – produites par différents ministères ou organismes – a longtemps été un point faible, conduisant à des doublons ou à des pertes d'information. Le Livre blanc sur la défense et la sécurité nationale de 2013 a donc prévu la création d'un comité interministériel de la prospective (CIP), présidé par le SGDSN. Tout en préservant la pluralité des sources d'analyse, le CIP, qui s'est réuni à l'automne 2015, veille à la cohérence des travaux de prospective dans le domaine de la sécurité et de la défense, et s'assure que les recommandations émises dans ce cadre sont suivies d'effets.

Contribuer à la sécurité des sites industriels sensibles fait partie des missions principales du SGDSN. D'autant plus que l'année 2015 a été marquée par deux attentats et actes malveillants contre des installations sensibles : le 26 juin, dans l'entreprise Air Products, à Saint-Quentin-Fallavier (Isère), et le 14 juillet, sur le site pétrochimique de LyondellBasell, à Berre-l'Étang (Bouches-du-Rhône).

Ces deux événements, qui confirment la vulnérabilité de certains sites industriels sensibles, ont conduit à mettre en œuvre plusieurs actions. Le SGDSN a ainsi piloté la réalisation d'un guide d'autoévaluation des vulnérabilités face aux actes terroristes ou malveillants. Celui-ci a été diffusé, dès juillet 2015, aux opérateurs responsables de ces sites. Une inspection systématique des sites Seveso a par ailleurs été ordonnée, sous la responsabilité des préfets, tandis qu'une mission interministérielle d'audit a rendu, à la fin de 2015, ses conclusions sur les moyens d'améliorer les enquêtes administratives « de criblage » pour l'accès aux sites sensibles des personnes extérieures à l'entreprise. Enfin, à la fin de l'année, le ministère de l'écologie a remis une étude en vue d'identifier les sites Seveso susceptibles d'être classés « points d'importance vitale ».

Dans le même esprit, le Premier ministre a confié au SGDSN le soin d'engager une réflexion interministérielle sur la sécurité des installations industrielles sensibles face aux malveillances. Les premiers résultats ont été remis au Premier ministre en novembre 2015 et les conclusions définitives au premier trimestre 2016.

DES EXERCICES POUR SE PRÉPARER AUX CRISES

Les exercices gouvernementaux sont l'un des moyens de préparer l'ensemble des acteurs à une crise majeure. Sur ce point, le SGDSN assiste le Premier ministre dans sa mission de préparation et de coordination de l'action des pouvoirs publics dans une telle situation. En 2015, deux exercices d'ampleur ont ainsi été réalisés.

Gaz 15 a simulé une rupture de l'approvisionnement en gaz de la France. L'exercice a permis de tester le « plan urgence gaz » (PUG), mais aussi de familiariser les acteurs de la cellule interministérielle de crise (voir ci-dessous) avec les mécanismes européens de coordination en la matière.

De son côté, Eurofoot 15 a permis de préparer l'Euro 2016, en testant notamment les prises de décisions spécifiques aux grands événements sportifs et l'articulation des dispositifs de l'État avec ceux des collectivités accueillant les matchs.

Le SGDSN a également coordonné les retours d'expérience de ces deux exercices, qui ont débouché sur l'élaboration de plans d'action interministériels.

Par ailleurs, un exercice franco-américain de réponse à un attentat biologique s'est également déroulé à Paris, en janvier 2015, sous le double pilotage du SGDSN et des services de la Maison-Blanche.

UNE CELLULE INTERMINISTÉRIELLE POUR FAIRE FACE AUX CRISES

La cellule interministérielle de crise (CIC) est l'outil du Premier ministre pour conduire l'action gouvernementale en matière de réponse aux crises majeures. Dans sa forme actuelle, elle est issue du livre blanc sur la défense et la sécurité nationale de 2008 et régie par une circulaire du Premier ministre de janvier 2012. Composée de trois cellules – décision, situation (synthèse, opérations, anticipation) et communication –, la CIC est un élément clé de la conduite opérationnelle d'une crise intervenant sur le territoire national.

La décision de l'activer revient au Premier ministre. Il désigne un ministre chargé de la conduite des opérations. Celui-ci active la CIC, avec l'ensemble des ministères concernés. Depuis 2008, un programme de professionnalisation est mis en œuvre, afin de renforcer la formation des personnels impliqués dans la mise en œuvre de la CIC et des plans gouvernementaux. Cette montée en compétences s'appuie notamment sur des séquences de formation, d'entraînement, d'exercices et de retours d'expérience, coordonnés par le SGDSN.

En 2015, deux exercices majeurs ont ainsi été menés à bien : Gaz 15, sur les difficultés d'approvisionnement en gaz naturel, et Eurofoot 15, pour préparer la tenue de cette grande manifestation sportive au printemps 2016 (voir la présentation de ces deux exercices ci-dessus). Au total, la CIC a été activée durant 49 jours au cours de l'année, ce qui constitue une durée très exceptionnelle.

RENFORCER LA FILIÈRE FRANÇAISE DE LA SÉCURITÉ

Installé en octobre 2013 par le Premier ministre, le comité de la filière industrielle de sécurité (CoFIS) regroupe onze ministres, des représentants des collectivités territoriales et du Parlement, des dirigeants de sociétés développant ou utilisant des solutions de sécurité, des présidents de pôles de compétitivité, ainsi que des chercheurs issus du monde académique. L'objectif est de structurer cette filière, de renforcer sa compétitivité et de l'aider à développer les technologies permettant de faire face aux menaces et aux risques pesant sur la vie de la Nation.

La première feuille de route du CoFIS, portant sur 2014 et 2015, a déjà permis plusieurs avancées. Parmi celles-ci, la réalisation de la première analyse du marché de la sécurité et des acteurs de la filière, ou encore la priorisation des besoins de cette dernière.

De même, le CoFIS a choisi et lancé plusieurs démonstrateurs sur des réalisations innovantes : plateforme public-privé de vidéoprotection, projet VOIE (vidéoprotection ouverte et intégrée), nouvelle génération de radiocommunications professionnelles sécurisées, projet PMR (système radio LTE résilient et offrant des capacités étendues aux acteurs de la sécurité)... La filière a également enregistré des premiers succès en matière de promotion des entreprises françaises à l'exportation ou en matière de standards internationaux.

En termes de visibilité de la filière, l'année a été marquée par la mise en ligne d'un site internet du CoFIS et par la mise en œuvre, à l'occasion du salon Milipol en novembre 2015, d'une action de communication sur le thème du marché de la sécurité.

UNE NOUVELLE FEUILLE DE ROUTE

Le 1er décembre 2015, le comité directeur du CoFIS s'est réuni sous la coprésidence du ministre de l'intérieur et du ministre de l'économie, de l'industrie et du numérique. À cette occasion, il a adopté une nouvelle feuille de route 2016-2017. Celle-ci prévoit d'associer toutes les parties prenantes publiques et privées – et notamment les petites et moyennes entreprises (PME) et les acteurs locaux –, en vue de déployer une véritable politique industrielle de sécurité.

Ce comité directeur s'étant tenu peu après les attentats du 13 novembre, il a également lancé deux initiatives : d'une part, la création d'une « Task Force de solidarité citoyenne », mobilisable en cas de situation exceptionnelle, et qui mettrait à disposition, sur une base volontaire, des compétences industrielles susceptibles de s'engager aux côtés des pouvoirs publics ; d'autre part, la proposition de consacrer une partie du troisième volet du Plan d'investissement d'avenir (PIA3), qui doit être lancé en 2017, à des investissements dans le domaine de la sécurité.

QUESTION DE FINANCEMENT

Le SGDSN participe au financement des projets de sécurité et de cybersécurité, via l'Agence nationale de la recherche (ANR) et le Fonds unique interministériel (FUI). En 2015, il a consacré 1,4 million d'euros au développement de trois projets destinés à permettre la neutralisation de drones. Il finance également en propre le développement de nouvelles solutions de lutte contre les menaces nucléaires, radiologiques, biologiques, chimiques et explosives. Enfin, le SGDSN mène une action de promotion des intérêts français, dans le cadre du programme européen Horizon 2020.

Protég

er

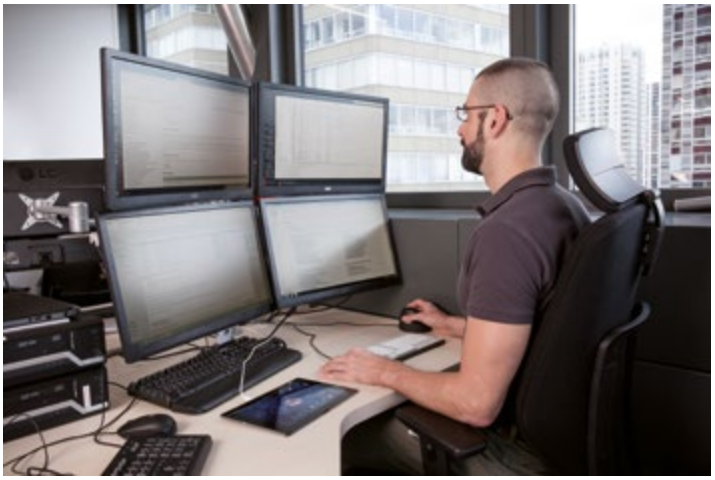
Sécuriser
les systèmes d'information

L'omniprésence des technologies de l'information dans la vie sociale et économique va de pair avec un accroissement de l'exposition aux attaques de toutes sortes sur les systèmes d'information. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est au cœur de la stratégie française de réponse à ces menaces et joue un rôle d'autorité, d'accompagnateur, mais aussi d'acteur opérationnel dans un domaine en pleine expansion, que l'État souhaite voir muer en véritable atout économique et stratégique national.

LA RECHERCHE AU SERVICE DE L'EXPERTISE DE L'ANSSI

L'ANSSI bénéficie de l'expertise technique et scientifique de ses six laboratoires, compétents en matière de cryptographie, de sécurité des composants, de sécurité des technologies sans fil, d'architectures matérielles et logicielles, de réseaux et protocoles, et de techniques de détection d'attaques. Structures de recherche à part entière, ils forment la base technologique de l'agence et jouent un rôle d'appui technique pour tous les autres services de l'ANSSI. Exemple de ce rôle, le laboratoire « sécurité des technologies sans fil » a participé aux audits de sécurité d'infrastructures dépendant des opérateurs télécoms, au côté du centre opérationnel de la sécurité des systèmes d'information (COSSI). Les laboratoires de l'ANSSI entretiennent la dynamique de recherche et de conseil par des publications régulières, lors de colloques et de congrès spécialisés (quarante articles en 2015), mais aussi en tissant des liens étroits avec le monde académique. En témoigne la création en 2015 du laboratoire d'exploration et de recherche en détection (LED), en étroite collaboration avec l'École normale supérieure et l'INRIA. Ainsi, les laboratoires sont une interface entre l'ANSSI et des interlocuteurs extérieurs, qu'il s'agisse d'autres organismes de recherche, d'acteurs industriels ou de partenaires internationaux, à l'instar du *Bundesamt für Sicherheit in der Informationstechnik* (BSI) allemand.

DES SYSTÈMES D'INFORMATION TOUJOURS PLUS SÛRS



Les différentes crises de l'année 2015 ont confirmé le besoin pour l'État de disposer d'outils de communication fiables et sécurisés. L'ANSSI contribue à répondre à ce besoin, en participant notamment à l'installation et au soutien des réseaux et terminaux sécurisés, comme le système de visioconférence Horus ou le réseau téléphonique Rimbaud. L'année 2015 a été marquée par la montée en puissance de l'intranet sécurisé interministériel pour la synergie gouvernementale (Isis), homologué au niveau « Confidentiel Défense ».

Cette évolution est notamment caractérisée par le remplacement par Isis de la messagerie sécurisée Magda, utilisée par les préfectures. Au total, pas moins de 500 nouveaux terminaux ont été installés, en collaboration avec le centre de transmissions gouvernemental (CTG).

En plus de ces technologies réservées aux services de l'État, l'ANSSI travaille également à des solutions utilisant des terminaux vendus dans le commerce. C'est l'objectif du projet Secdroid, un système sécurisé, fondé sur l'architecture Android, fonctionnant aussi bien sur smartphone que sur tablette. Une expérimentation poussée de ce système a été menée en 2015, en collaboration avec la gendarmerie nationale, dans le département du Nord.

Pour le compte de l'État, L'ANSSI a acquis auprès de la société Prim'X une licence globale pour l'utilisation d'un ensemble de logiciels de sécurité qualifiés. Cette opération inédite permet à la fois de rationaliser l'investissement public et d'encourager les administrations à utiliser un produit de confiance, sans autre coût que celui de sa maintenance.

L'ANSSI s'engage également auprès des entreprises, en les conseillant en matière de protection, en conduisant des audits de leurs systèmes les plus critiques, à leur demande, et en les assistant lorsqu'une crise de grande ampleur survient.

LES SOLUTIONS DE SÉCURITÉ PASSÉES AU CRIBLE

Afin de favoriser le développement d'une culture de la cybersécurité, auprès des administrations comme des entreprises, l'ANSSI assure une mission de certification et de qualification de produits. En 2015, 88 produits ont ainsi été certifiés « critères communs » (CC) par l'agence, selon la norme internationale ISO 15408, reconnue par la plupart des pays industrialisés. Parallèlement, l'agence délivre des certifications de premier niveau (CSPN, huit en 2015), strictement nationales, qui constituent une alternative plus rapide et moins coûteuse à la certification « critères communs ».

Si ces certifications garantissent la conformité technique d'un produit à un cahier des charges précis, elles ne valent pas recommandation de l'ANSSI quant à leur usage. Inversement, les produits qualifiés sont évalués très en amont par les techniciens de l'agence et répondent à un besoin de sécurité avéré. Une fois certifiés, ces produits (treize en 2015) peuvent faire l'objet d'une seconde évaluation, en vue d'un agrément de l'Otan ou de l'Union européenne.

Ce processus de contrôle s'applique également aux prestataires en audits de sécurité des systèmes d'information (Passi), qui font désormais l'objet d'une évaluation poussée, menée par des centres indépendants, eux-mêmes régulièrement évalués selon des critères fixés par l'ANSSI. En 2015, cette qualification a été accordée à neuf Passi. Du fait de la demande croissante en la matière, l'ANSSI a également lancé une phase expérimentale de qualification de prestataires de confiance dans trois autres domaines (détection d'incidents, réponse à incident, informatique en nuage), avec pour objectif de passer à la phase opérationnelle en 2016.

LA LOI DE PROGRAMMATION MILITAIRE ET LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

La publication de trois décrets d'application de la loi de programmation militaire 2014-2019 (LPM) a considérablement fait évoluer le cadre réglementaire de la sécurité des systèmes d'information. Désormais, les opérateurs d'importance vitale (OIV) ont l'obligation d'appliquer des mesures particulières de protection et de rendre compte de tous les incidents auxquels ils sont confrontés. La LPM répond également à la hausse prévisible de la demande d'audits de sécurité, en encadrant la définition de prestataires d'audits de SSI de confiance. Toutefois, les conditions concrètes d'application de la loi aux différents OIV dépendent encore de l'élaboration des arrêtés sectoriels, qui prendront en compte les particularités de chacun des secteurs concernés. Les services de l'ANSSI mènent, depuis octobre 2014, des discussions avec tous les acteurs (ministères et OIV), afin d'aboutir à des dispositions adaptées aux situations rencontrées.

LE SOUTIEN AUX ENTREPRISES DE CYBERSÉCURITÉ

Volet important de la stratégie nationale pour la sécurité du numérique – telle qu'elle a été présentée par le Premier ministre le 16 octobre 2015 –, la promotion de l'industrie de la cybersécurité française relève également des responsabilités de l'ANSSI. Grâce à sa participation à de nombreuses rencontres bilatérales et multilatérales (Forum international de la cybersécurité, Assises de la sécurité et des systèmes d'information…), l'agence est en mesure de sonder en permanence l'écosystème du secteur, d'en connaître les principaux acteurs et d'en identifier les manques, ce qui lui permet aussi de promouvoir les solutions de confiance, certifiées ou qualifiées par ses services.

Elle contribue par ailleurs directement au développement de l'offre, en pilotant la solution industrielle « Confiance numérique », dans le cadre de la seconde phase de la « Nouvelle France industrielle », un ensemble de plans de réindustrialisation, lancé par le Président de la République en 2013. Parmi les objectifs, le développement des acteurs nationaux du secteur, mais aussi la promotion de leur offre, notamment avec le lancement du label France Cybersecurity.

Enfin, l'agence met à disposition son expertise, en apportant, par exemple, son soutien au Commissariat général à l'investissement pour le Programme d'investissements d'avenir. Elle est aussi en contact direct avec les entreprises innovantes, qu'il s'agisse de PME – comme en témoigne le renouvellement, en 2015, de son partenariat avec Oséo – ou de groupes industriels, tels Thalès ou Airbus, qui ont mis en place des solutions issues des avancées du projet CLIP, système d'exploitation sécurisé sur une base Linux, développé par les laboratoires de l'ANSSI.

LA CULTURE DE LA SÉCURITÉ

Promouvoir la cybersécurité passe également par une politique ambitieuse de communication, notamment afin de faire prendre conscience des enjeux à tous les acteurs, quelle que soit leur nature. Si les grands acteurs sont sensibilisés à cette nécessité, un effort particulier est consacré aux PME et aux particuliers, moins au fait de ces problématiques. La publication d'un *Guide des bonnes pratiques de l'informatique*, coédité avec la Confédération générale des petites et moyennes entreprises (CGPME), ou le lancement de la campagne #Cybervigilant, qui rappelle les précautions élémentaires, répondent à cette préoccupation.

L'action de formation menée par l'agence contribue à cette diffusion nécessaire d'une véritable culture de la sécurité. Le centre de formation à la sécurité des systèmes d'information (CFSSI) a ainsi accueilli, en 2015, 1 450 stagiaires, tous agents de l'État, pour des stages allant de l'initiation au perfectionnement. Il dispense par ailleurs une formation de treize mois, sanctionnée par un titre d'expert en sécurité des systèmes d'information (huit diplômés du CFSSI en 2015). Il porte également CyberEdu, un projet de production de modules « clés en main », à destination des enseignants et destinés à promouvoir l'apprentissage de la cybersécurité dans l'enseignement supérieur.

LA RÉPONSE AUX INCIDENTS

En dernier recours, en cas d'attaque avérée ou soupçonnée, le centre opérationnel de la sécurité des systèmes d'information (COSSI) assure la défense des services de l'État et des opérateurs privés les plus sensibles, qu'ils figurent ou non parmi les OIV. Pour mener à bien sa mission, il met en œuvre des dispositifs de veille et de détection, notamment par le biais de sondes sur les réseaux, et par la collecte et l'analyse des vulnérabilités et des codes malveillants qui les exploitent. En 2015, plus de 2 300 codes malveillants ont ainsi été identifiés. Le COSSI traite également tous les signalements d'incidents que lui soumettent les différents opérateurs (4 000 en 2015) et évalue les dégâts éventuels. En cas d'attaque de grande envergure, comme celle qui a affecté TV5 Monde, il est en capacité de mettre en place une cellule de crise pour répondre à l'urgence de la situation, ce qui est également le cas dans le cadre d'événements exceptionnels (attentats de janvier et de novembre 2015, accident du vol de la Germanwings, COP21). Dans un cadre préventif, il est également chargé de mener des audits des systèmes dépendant de l'État et des OIV.

LE DIALOGUE À TOUS LES ÉCHELONS

Par nature, l'univers des systèmes d'information ne connaît pas de frontières. Pour cette raison, l'ANSSI est dans l'obligation d'inscrire son action dans une logique de coordination avec tous les acteurs concernés, PME régionales ou grandes institutions internationales. L'agence a donc décidé en 2015 de déployer un dispositif d'action territoriale, seul moyen de toucher des structures moins préparées en matière de cybersécurité que les OIV ou les administrations, interlocuteurs historiques de l'ANSSI. En 2015, quatre régions (Île-de-France, Hauts-de-France, Bretagne et Auvergne-Rhône-Alpes) ont ainsi vu la nomination d'un coordonnateur régional, chargé de décliner les services de l'agence au niveau local.

À l'autre extrémité du spectre, l'ANSSI porte la parole de la France dans toutes les institutions internationales concernées par la sécurité des systèmes d'information (Union européenne, Otan, ONU, OCDE) sur des sujets allant de la coopération interétatique à la définition de normes techniques, en passant par la reconnaissance mutuelle des certifications et qualifications. Cet investissement constant de la France sur le thème de la cybersécurité lui permet de faire valoir une expertise et une légitimité indéniables, ce qui lui vaut de peser efficacement sur les discussions en cours. L'accord politique donné par l'Union européenne, en 2015, à la directive *Network & Information Security* (NIS), dont la philosophie est très proche de la loi de programmation militaire 2014-2019, est une illustration de cette capacité d'influence.

Cont

trôler Certifier

Contrôler les exportations d'armement et veiller sur le transfert des technologies sensibles, lutter contre les risques de prolifération, contrôler les exploitants de données spatiales ou encore assurer la cohérence des actions menées en matière de politique de recherche scientifique et de projets technologiques intéressant la défense et la sécurité nationale… : l'action du SGDSN intègre une importante dimension internationale et s'appuie sur une forte capacité de coopération.

La menace évolue. Les moyens de l'évaluer et de la contrer aussi. Face aux enjeux géostratégiques et de sécurité internationale, le SGDSN agit sur plusieurs fronts, afin de maîtriser les transferts de technologies les plus sensibles et de répondre aux enjeux stratégiques liés à la prolifération et à la maîtrise des armements de toute nature, à la sécurité européenne et à la lutte contre les flux illicites.

SÉCURITÉ ET LUTTE CONTRE LA PROLIFÉRATION

Dans le domaine de la lutte contre la prolifération des armes de destruction massive, la France agit dans un cadre multilatéral et au travers d'initiatives spécifiques. Son objectif est triple : répondre aux situations de crise, participer au renforcement du cadre normatif international de non-prolifération, entraver les transferts sensibles illégaux et lutter contre les réseaux clandestins. Dans ce contexte, le SGDSN joue un rôle d'animateur et de coordonnateur interministériel du dispositif national de lutte contre la prolifération. Il assure la coordination de la réponse nationale aux interceptions réalisées dans le cadre de la *Proliferation Security Initiative* (PSI), directement ou avec le concours de partenaires étrangers. La fréquence de ces interceptions ne cesse de croître depuis la mise en œuvre de la PSI. Dix-sept affaires d'interception de « biens proliférants » ont ainsi été menées dans ce cadre, de mi-2014 à mi-2015, soit le double de l'année précédente.

UN CONSEIL POUR LA BIOSÉCURITÉ

Face à la menace du risque chimique ou bactériologique, le Premier ministre a mis en place, en 2015, le Conseil national consultatif pour la biosécurité (CNCB). Sa mission : éviter le détournement des recherches sensibles à des fins terroristes. Le pilotage de cette nouvelle instance a été confié au SGDSN. Le conseil s'est réuni pour la première fois le 30 novembre. Il sera chargé, notamment, de proposer des mesures propres à assurer la prévention et la détection d'éventuelles menaces, leur traitement et l'information du public. Il mènera des travaux de veille et de prospective sur les recherches à caractère dual – utilisation civile et militaire d'une même technologie – et formulera des recommandations, afin que les progrès réalisés dans les sciences du vivant ne génèrent pas de menaces nouvelles.

LA PROTECTION DES PROGRAMMES SPATIAUX

Le SGDSN assure la synthèse des positions françaises relatives à la sécurité des programmes spatiaux européens de navigation par satellite (Galileo et Egnos) et de surveillance de la Terre (Copernicus). En 2015, les travaux pilotés par le SGDSN ont permis de fixer, en liaison avec les États partenaires et la Commission européenne, les normes minimales communes définissant les règles d'utilisation du signal *Public Reglemented Service* (PRS), émis par le satellite Galileo. La finalisation de ces normes communes ouvre la voie aux négociations d'accès des pays tiers à Galileo et au signal PRS. Les deux premiers pays candidats sont les États-Unis d'Amérique et la Norvège.

Par ailleurs, en 2015, le SGDSN a assuré la coordination interministérielle, lors de l'élaboration de la position française relative à la proposition de directive européenne sur le contrôle des images spatiales.

(...) Le SGDSN apporte un soutien et une expertise technique pour des missions et des sujets très politiques

3 questions à
JEAN-LOUIS FALCONI
DIPLOMATE, JEAN-LOUIS FALCONI EST DIRECTEUR DES AFFAIRES INTERNATIONALES, STRATÉGIQUES ET TECHNOLOGIQUES AU SGDSN.

Comment caractériser l'activité internationale du SGDSN ?
C'est un positionnement particulier, qui n'a pas beaucoup d'équivalents à l'étranger. Nous sommes d'abord une instance de coordination interministérielle qui permet de définir, sur certains sujets de sécurité particulièrement complexes, le message que la France doit porter vis-à-vis de partenaires étrangers, mais ce message peut être aussi porté par d'autres ministères que nous. Dans certains cas, où nous recevons un mandat du Président de la République ou du Premier ministre, nous sommes les seuls négociateurs comme on l'a vu dans l'affaire des BPC Mistral avec la Russie.

Quelles sont les missions du SGDSN en la matière ?
Le SGDSN apporte un soutien et une expertise technique pour des missions et des sujets très politiques, qui ont trait aux missions régaliennes de l'État, comme les exportations de matériels de guerre ou la lutte contre la prolifération nucléaire, chimique, biologique (NRBC). Le secrétaire général est parfois, sur certains sujets sensibles, l'interlocuteur unique des autorités étrangères. Nous synthétisons les analyses des services de renseignement pour évaluer la menace terroriste en France et à l'égard de nos intérêts à l'étranger. Notre travail comporte une importante dimension de prospective et d'anticipation.

Dans votre domaine, que peut-on retenir de l'année 2015 ?
Je retiendrai la mise en évidence du rôle du SGDSN dans de grands dossiers à la fois industriels, stratégiques et politiques : l'encadrement gouvernemental de la fusion Nexter-KMW, qui est d'abord un succès franco-allemand, l'affaire des BPC Mistral ou les évolutions d'Areva, et le suivi des prospects de cette entreprise à l'exportation, en lien avec la sécurité nationale. Nous essayons de pousser une dimension européenne de la sécurité. C'est le cas avec le programme de satellites Galileo ou la fluidification du marché européen des produits de défense avec nos partenaires des six pays de la LoI (Letter of Intent) et, plus largement, avec la Commission européenne. Enfin, dans le domaine de la lutte contre la prolifération, l'année 2015 a notamment vu l'installation du CNCB, le Conseil national consultatif pour la biosécurité.

PROTÉGER LE POTENTIEL SCIENTIFIQUE ET TECHNIQUE FRANÇAIS

Le SGDSN pilote la montée en puissance du dispositif de protection du potentiel scientifique et technique de la nation (PPST). À ce titre, il reçoit l'ensemble des demandes de création de zones à régime restrictif (ZRR), émanant des ministères concernés. Ces zones permettent de protéger l'accès aux savoirs, savoir-faire et technologies détenus par les établissements publics et privés conduisant des activités de recherche ou de production. Les efforts de sensibilisation des opérateurs (laboratoires de recherche, arsenaux militaires, entreprises...), réalisés par le SGDSN et par les ministères, contribuent à entretenir la dynamique de création des ZRR (451 créées à ce jour).

CONTRÔLER LES EXPORTATIONS SENSIBLES

La France exerce un contrôle strict sur les exportations de matériels de guerre et matériels assimilés, conformément aux impératifs de sa politique nationale en la matière, mais aussi à ses engagements internationaux. Le régime de contrôle de ces exportations repose sur des décisions prises par le Premier ministre, sur avis de la commission interministérielle pour l'étude des exportations de matériels de guerre (CIEEMG). Présidée par le secrétaire général de la défense et de la sécurité nationale, cette instance est composée des ministères chargés de la défense, des affaires étrangères et de l'économie. Depuis 2014, les exportations font l'objet d'un contrôle par licence unique, délivrée par le ministre chargé des douanes, après avis du Premier ministre, des ministres chargés de l'économie, des affaires étrangères et de la défense, dans le cadre de la CIEEMG. En 2015, La commission, réunie en session plénière, a examiné 312 dossiers, et prononcé 205 avis favorables et 107 avis défavorables, sans tenir compte des 6 000 demandes qui ont fait l'objet d'un traitement dématérialisé en procédure continue.

Par ailleurs, le SGDSN participe activement aux travaux internationaux sur le transfert intracommunautaire et le contrôle à l'exportation des matériels de guerre ou assimilés. Il anime le sous-comité export de l'accord-cadre LoI (*Letter of Intent*), chargé de l'harmonisation et de la simplification des procédures applicables aux transferts entre les six principaux pays producteurs d'armement en Europe (Allemagne, Espagne, France, Italie, Royaume-Uni et Suède). En 2015, le SGDSN a été force de proposition avec ses partenaires de la LoI dans l'élaboration et la diffusion d'un *Position Paper* qui définit de nouveaux axes pour une mise en œuvre plus efficace de la directive transferts intracommunautaires entre États membres (définition des produits spécifiquement destinés à un usage militaire, harmonisation des conditions de réexportation des équipements de défense, certification des entreprises…). Ces travaux ont servi de base aux recommandations de la Commission européenne, présentées à la fin de l'année 2015. Ils devraient également constituer le socle du rapport qui sera remis au Conseil européen en 2016.

LE DOUBLE USAGE DES TECHNOLOGIES SENSIBLES

Le SGDSN participe à l'établissement de la position technique française, au sein de plusieurs instances internationales, dans le cadre de négociations et de partenariats concernant le commerce des biens et des technologies à double usage. Ces derniers font l'objet d'une liste régulièrement mise à jour, afin de tenir compte de l'évolution des technologies et de leur disponibilité sur le marché international. Cette liste reprend celles des biens à double usage, visés par l'Arrangement de Wassenaar, le NSG (groupe des fournisseurs nucléaires), le MTCR (régime de contrôle de la technologie des missiles), le groupe Australie (contre la prolifération biologique et chimique) et la Convention d'interdiction des armes chimiques.

En 2015, la commission interministérielle des biens à double usage (CIBDU) a mandaté le SGDSN pour conduire l'instruction, au sein de ces différentes instances, de dossiers jugés particulièrement sensibles pour des motifs techniques, politiques ou en raison de l'impact sur l'emploi ou le tissu industriel local.

LES MANDATS

Le SGDSN se voit confier par le Président de la République et le Premier ministre des mandats d'analyse et de proposition sur des questions relevant de ses compétences. En 2015, le SGDSN a mené des travaux conjointement avec les ministères et divers organismes comme l'Agence des participations de l'État ou le Commissariat à l'énergie atomique et aux énergies renouvelables, dans plusieurs domaines comme la préservation des compétences rares ou l'avenir des filières stratégiques (nucléaire, électronique…).

NÉGOCIATIONS INTERNATIONALES : DES BPC À KANT

SÉCURISER LES TRANSMISSIONS

Le SGDSN abrite une structure particulière : le centre de transmissions gouvernemental (CTG), une unité militaire mise pour emploi auprès du secrétariat général. Il est chargé d'assurer les transmissions interministérielles sécurisées et de mettre à la disposition du Président de la République des moyens de communication protégés, notamment lors de ses déplacements à l'étranger. Depuis 2015, le SGDSN assure la gestion administrative du CTG. Au mois de décembre 2015, le CTG a déployé et exploité une installation de communications sécurisées sur le site du Bourget, à l'occasion de la COP21. Par ailleurs, pendant six mois, le centre a exploité avec succès son site de secours durant les travaux réalisés dans la cage de Faraday, installée sur le site de l'Hôtel national des Invalides.

Dans le domaine de l'industrie de défense et de la coopération européenne, le SGDSN est également intervenu à l'occasion du rapprochement entre deux poids lourds de l'armement terrestre – le Français Nexter et l'Allemand Krauss-Maffei Wegmann (KMW) – à travers le projet Kant (KMW And Nexter Together). Officialisé en juillet 2015, ce rapprochement va au-delà du simple partage d'un programme d'armement. Il devrait aboutir à la naissance d'un nouvel acteur 100 % européen, doté d'une vision stratégique unifiée, notamment en matière d'exportation des équipements de défense terrestre.

Éclai

rer

Planifier

Anticiper les évolutions et les menaces, éclairer la décision des pouvoirs publics, actualiser en permanence les différents plans gouvernementaux touchant à la défense et à la sécurité, animer des travaux sur des questions soulevées par le développement des technologies et des usages : autant de missions assurées par le SGDSN. Et autant de sujets qui ont fortement mobilisé le secrétariat général en 2015.

Face à des risques qui évoluent et se transforment en permanence, l'État doit adapter régulièrement ses réponses pour préserver leur efficacité et anticiper de nouvelles menaces. L'un des instruments de cette capacité d'anticipation est le bureau de veille et d'alerte du SGDSN. Celui-ci fonctionne en continu, 7 jours sur 7 et 24 heures sur 24. Il travaille en étroite liaison avec les centres opérationnels des ministères. En 2015, ce dispositif a été systématiquement activé, en particulier lors des attentats.

RÉNOVATION DES PLANS GOUVERNEMENTAUX

La capacité d'anticipation s'inscrit également dans le moyen et le long terme. Elle passe alors par la rénovation et la mise à jour des plans gouvernementaux, qui est l'une des missions clés du SGDSN.

À ce titre, le secrétariat général a notamment travaillé, avec le pôle d'analyse du risque de la direction générale de l'aviation civile (Dgac), à une supervision des dispositifs d'évaluation du risque pour les vols en provenance de pays jugés sensibles et de lutte contre la menace des missiles sol-air de courte portée. Dans le même esprit, le SGDSN a animé la mission interministérielle sur l'usage des drones et remis au Premier ministre un rapport et des propositions sur le sujet (voir page 37).

Sur le long terme, il mène, finance ou anime également, depuis plusieurs années, des travaux sur la menace représentée par les explosifs artisanaux, utilisés à des fins terroristes, ou sur les scénarios de référence en matière de risques nucléaires, radiologiques, bactériologiques et chimiques (NRBC).

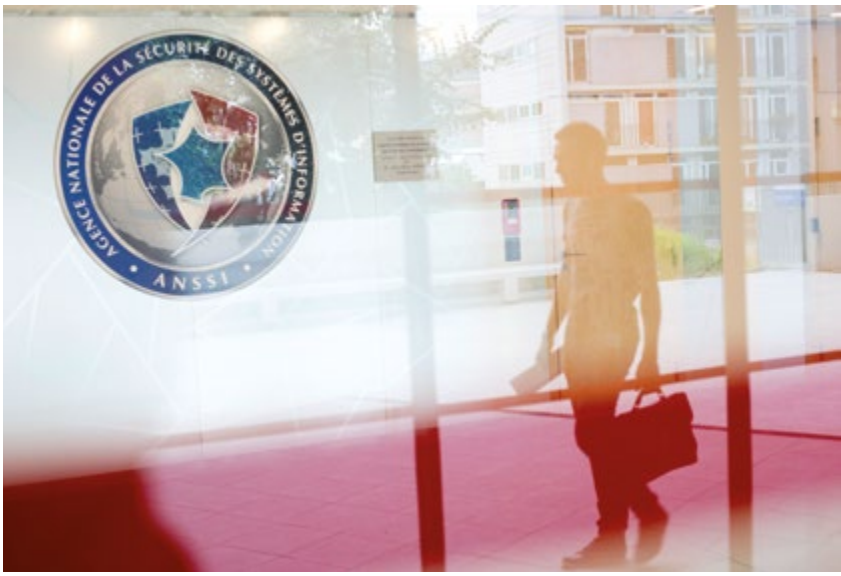
PCA : DES PLANS POUR ASSURER LA CONTINUITÉ DE L'ACTIVITÉ

Les plans de continuation de l'activité (PCA) doivent permettre aux administrations, services publics et entreprises de poursuivre leur activité en cas de crise majeure (sanitaire, technologique, environnementale...). Afin d'améliorer l'efficacité potentielle des PCA, le SGDSN a mandaté le haut fonctionnaire de défense et de sécurité (HFDS) des ministères économiques et financiers, en vue de développer une offre française de certification de ces dispositifs. Dans le même temps, le secrétariat général continue de soutenir les ministères dans la mise en place de leurs PCA et a engagé une démarche en vue de caractériser leurs besoins en spécialistes de la sécurité des systèmes d'information.

RÉVISION DES DIRECTIVES NATIONALES DE SÉCURITÉ

Les directives nationales de sécurité (DNS) restent toutefois le principal outil de renforcement de la politique de sécurité des activités d'importance vitale (SAIV). Chacune d'elle couvre un champ très large et transversal, intégrant notamment la planification de la continuité des activités face à un large éventail de risques potentiels, mais aussi le renforcement de la sécurité des systèmes d'information, en étroite liaison avec l'ANSSI. La mise à jour de ces documents représente un enjeu important, face à des menaces qui se démultiplient.

En 2015, six DNS ainsi rénovées ont été approuvées. Elles portent respectivement sur les communications électroniques et internet, l'électricité, le gaz, les hydrocarbures, les produits de santé et le transport aérien. Dans le même temps, la révision de onze autres DNS a été engagée au cours de l'année.



VIGIPIRATE : UN OUTIL CLÉ RÉACTUALISÉ

Par la présence accrue des forces de sécurité dans l'espace public et ses implications sur la vie quotidienne, le plan Vigipirate, placé sous l'autorité du Premier ministre, est le plus visible des dispositifs de protection contre la menace terroriste. Apparu – sous des formes moins élaborées – au début des années 1990, il vise un triple objectif :

• assurer en permanence une protection adaptée des citoyens, du territoire et des intérêts de la France contre la menace terroriste ;

• développer et maintenir une culture de la vigilance, afin de prévenir ou de déceler toute menace d'action terroriste le plus en amont possible ;

• permettre une réaction rapide et coordonnée des services de l'État, en cas de menace caractérisée ou d'action terroriste, et assurer la continuité des activités d'importance vitale.

Un nouveau plan Vigipirate a été publié en 2014. Les améliorations ont porté sur la lisibilité du dispositif pour le public et sur un renforcement de l'évaluation de la menace terroriste et un pilotage plus précis des mesures de protection. Après les attentats de janvier 2015, ses postures ont fait l'objet d'une évaluation, puis d'une actualisation permanente, afin de l'adapter au contexte.

VINGT-SIX POSTURES VIGIPIRATE DIFFUSÉES EN 2015

Le plan Vigipirate comprend un ensemble d'environ 300 mesures, réparties entre un socle de mesures permanentes dans douze grands domaines et une série de mesures additionnelles, activées en fonction de l'évolution de la menace. Il est organisé en une partie publique – informant la population des mesures de protection et de vigilance, et mobilisant tous les acteurs – et une partie classifiée, destinée aux pouvoirs publics et aux opérateurs d'importance vitale.

Dans le contexte particulier de 2015, le SGDSN a ainsi diffusé vingt-six postures Vigipirate (modifications du dispositif), contre un rythme habituel de quatre ou cinq par an.

Outre Vigipirate, le SGDSN participe également à l'actualisation d'autres plans. Après la révision du plan Piratair-Intrusair (réponse à des actes illicites mettant en jeu la sûreté ou la souveraineté aérienne), à la fin de 2014, il a engagé en 2015, avec l'ANSSI, la rénovation du plan Piranet (réponse à des attaques sur les systèmes d'information).

UN PLAN CONTRE EBOLA

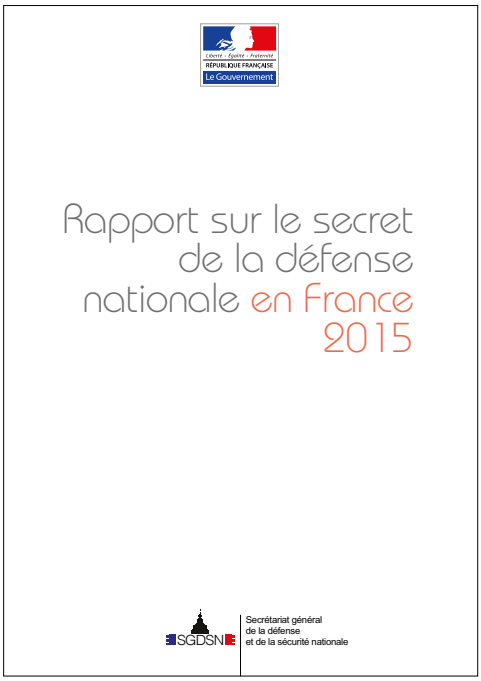
En matière de prévention des risques, le rôle du SGDSN ne se limite pas au terrorisme. Le secrétariat général a ainsi coordonné les travaux interministériels d'élaboration du nouveau plan de prévention et de lutte contre la maladie Ebola. Publié en novembre 2014, ce plan organise la réponse face à d'éventuels cas importés sur le territoire national et prévoit la prise en charge des ressortissants français ou binationaux qui pourraient être atteints dans les pays touchés par l'épidémie.

Indispensable à la sauvegarde des intérêts de la Nation, le secret de la défense nationale est un instrument au service de l'État de droit. Sa mise en œuvre est encadrée par la loi. Elle est soumise au contrôle du juge constitutionnel

UN RAPPORT SUR LE SECRET DE LA DÉFENSE NATIONALE

Pour la première fois, le SGDSN a élaboré et publié un rapport sur le secret de la défense nationale en France en 2015. Le secrétariat général est en effet chargé de concevoir et de faire respecter les mesures de protection de ce secret.

Accessible à tous sur le site du SGDSN, le rapport présente les explications et les données statistiques sur le secret de la défense nationale. Depuis 1981, il existe ainsi trois niveaux de classification selon la nature des données : « Confidentiel Défense », « Secret Défense » et « Très Secret Défense ». Au 1er janvier 2015, on dénombrait 288 334 documents classifiés au niveau « Secret Défense », répertoriés dans un inventaire centralisé. À cette même date, 50 % de ces documents relevaient du ministère chargé de l'énergie – en raison des thématiques liées à l'énergie nucléaire, aux installations sensibles et à la sécurité des transports –, 44 % du ministère de la défense, 4 % de celui de l'intérieur et 2 % des autres ministères.



HABILITATION ET DÉCLASSIFICATION

Pour accéder à ces documents classifiés, il faut remplir une double condition : avoir besoin d'en connaître le contenu (condition appréciée par l'autorité hiérarchique) et avoir été habilité au préalable, après une enquête administrative. Au 1er janvier 2015, 413 235 personnes étaient habilitées à ce titre, soit une personne sur 160 habitants. Les personnes habilitées relèvent à 70 % du ministère de la défense, 13 % de celui de l'énergie et 12 % de celui de l'intérieur. Compte tenu des changements de postes, 20 % de ces autorisations sont renouvelées chaque année.

L'accès du public à un document classifié n'est possible qu'après la déclassification de ce dernier et au terme d'un délai de cinquante ans, voire de cent ans. Des dérogations sont toutefois possibles : le Président de la République a ainsi décidé la déclassification des documents relatifs à la Seconde Guerre mondiale et le SGDSN a reçu la mission de travailler à la déclassification des archives relatives à l'intervention de la France au Rwanda entre 1990 et 1994.

PROTECTION JURIDIQUE ET PROTECTION PHYSIQUE

La protection des documents classifiés ne se limite pas à l'apposition d'un tampon « Secret Défense ». Tous les documents classifiés doivent en effet être conservés dans une armoire forte, elle-même située dans une zone sécurisée (local ou emplacement à l'accès réglementé et faisant l'objet de mesures de protection matérielle). Avec l'ANSSI, le SGDSN travaille également à la sécurisation des données dématérialisées.

ESSOR DES DRONES : ENJEUX ET MENACES

En 2015, le SGDSN a animé les travaux interministériels d'élaboration d'un rapport sur l'essor des drones aériens civils en France. Ces travaux se sont notamment appuyés sur les conclusions d'un colloque organisé par le secrétariat général au Conseil économique, social et environnemental, le 28 mai 2015. Le rapport correspondant a été remis au Parlement en octobre. La nécessité de cette réflexion d'ensemble résulte de la multiplication des survols de zones sensibles, d'incidents sur le partage de l'espace aérien, mais aussi de la miniaturisation croissante des drones, qui les rend de plus en plus difficiles à détecter, notamment la nuit. Il était donc indispensable de revoir la réglementation des drones, qui remontait à des arrêtés d'avril 2012.

Le rapport remis au Parlement dresse un état des lieux. Il évalue le parc des drones en France autour de 200 000 unités, dont 98 % pèsent moins de deux kilos. Ce parc est en rapide expansion et couvre à la fois des usages professionnels (médias, production audiovisuelle, surveillance d'ouvrages d'art et d'installations techniques, agriculture...) et des usages grand public.

Comme nombre d'activités, ces usages sont porteurs de différents risques : accidents, actes malveillants (captations d'informations, utilisation comme armes), mais aussi atteinte à la crédibilité des pouvoirs publics, des institutions ou des entreprises.

SÉCURISER LE MARCHÉ SANS L'ENTRAVER

Il ne s'agit pas pour autant d'entraver le développement de ce marché, mais plutôt de « créer les conditions favorables au développement d'une filière créatrice d'emplois et de richesse, tout en luttant plus efficacement contre les infractions commises par les télépilotes, professionnels ou non ».

Pour cela, le rapport du SGDSN formule un ensemble de préconisations portant sur trois grandes thématiques. D'une part, l'évolution du cadre juridique, dans le sens d'une plus grande responsabilisation des télépilotes. D'autre part, l'adaptation des moyens de détection des usages malveillants, d'identification des drones concernés et de leurs télépilotes et – si nécessaire – de neutralisation des engins présentant une menace. Enfin, le développement des coopérations internationales – en particulier avec l'Organisation de l'aviation civile internationale (OACI) –, en vue d'harmoniser le cadre réglementaire et de mutualiser des programmes de recherche.

DE LA RÉFLEXION AUX ACTES

Le rapport du SGDSN a entraîné une adaptation de la réglementation applicable, matérialisée par la publication de deux arrêtés signés le 17 décembre 2015. Le premier porte sur la conception des drones civils, les conditions de leur emploi et les capacités requises de la part de leurs utilisateurs. Le second précise les conditions d'insertion des drones dans l'espace aérien.

RESSOURCES

Finances, gestion des ressources humaines, logistique, infrastructures, achat public, sécurité des personnes et des locaux... Toutes ces fonctions de soutien sont essentielles au SGDSN pour en assurer le bon fonctionnement et lui permettre d'accomplir l'ensemble de ses missions.

RENFORCER LES INFRASTRUCTURES

Plusieurs chantiers majeurs se sont déroulés en 2015 comme la rénovation du poste de sécurité de l'Hôtel national des Invalides. Ces travaux ont notablement amélioré les conditions de travail des gendarmes et la relation avec les usagers du bâtiment. Face aux besoins croissants de stockage de l'ANSSI et du CTG, le SGDSN a mobilisé de nouveaux locaux sur la base aérienne de Villacoublay (150 m² en 2015) et sur le site des Invalides (330 m² aménagés en 2016).

Par ailleurs, au mois d'octobre, le SGDSN a lancé le projet HNI 2018 (Hôtel national des Invalides). Celui-ci s'inscrit dans le cadre du schéma directeur immobilier pluriannuel et répond au besoin de réaménagement des locaux du HNI, afin d'assurer la montée en puissance de l'ANSSI, et aux évolutions de fonctionnement des autres directions.

L'INNOVATION SOCIALE AU RENDEZ-VOUS

L'année 2015 a été marquée par une activité intense dans le domaine des ressources humaines avec près de 500 mouvements de personnel (274 arrivées et 211 départs) et la transformation d'une cinquantaine de contrats à durée déterminée en CDI. Le SGDSN regroupe actuellement environ 900 personnes. L'offre et le volume des formations se sont accrus, notamment au profit de l'ANSSI, pour un budget de 400 000 euros accordé à cette activité, et l'élargissement des offres proposées. Au-delà des chiffres, le SGDSN fait de l'innovation sociale l'une de ses priorités. Le déploiement du processus Pass (parcours d'accompagnement vers la suite du SGDSN), lancé en 2014, s'est poursuivi cette année. Ce dispositif est destiné principalement au personnel non titulaire de l'ANSSI, en fin de contrat. Il permet de préparer une reconversion professionnelle, à l'issue d'un passage par l'agence. Autre innovation : la meilleure prise en compte des risques psychosociaux, en application des directives gouvernementales en la matière.

SÉCURITÉ ET MAÎTRISE BUDGÉTAIRE

Le SGDSN s'est doté d'une charte de gestion qui fixe les modalités du pilotage budgétaire, en améliorant sa qualité et sa clarté. L'application de ces procédures a participé à la bonne réalisation de l'ensemble des missions du SGDSN, à l'optimisation de l'utilisation des crédits et au respect des exigences de la commande publique. Par ailleurs, l'activité 2015 a été marquée par la réalisation de plusieurs audits et contrôles externes : un contrôle de l'ANSSI par la Cour des comptes, un audit de la chaîne de la dépense par les services du Premier ministre, ou encore une mission de conseil menée par l'inspection générale des finances, qui ont tous témoigné du haut niveau de performance atteint par le SGDSN en matière de soutien administratif.

(...) les actions de formation restent une priorité pour l'ensemble des agents.

3 questions à
PATRICIA COSTA
COMMISSAIRE GÉNÉRAL DE PREMIÈRE CLASSE, PATRICIA COSTA DIRIGE LE SERVICE DE L'ADMINISTRATION GÉNÉRALE DU SGDSN.

Quel est le rôle de votre service ?
Le service de l'administration générale intervient au profit de l'ensemble des directions du SGDSN et des organismes qui lui sont rattachés. Il réalise des missions transversales portant sur les activités administratives, financières et logistiques. Il est chargé en outre de la sécurité. En 2015, le service a particulièrement veillé à l'accompagnement de la montée en puissance de l'ANSSI et assuré la prise en charge du centre de transmissions gouvernemental (CTG), tout en maintenant un haut niveau de compétence dans ses missions habituelles, comme la programmation budgétaire, la commande publique, la logistique – dont l'infrastructure –, ou encore la gestion des ressources humaines.

Justement, quels sont les principaux enjeux liés à la gestion des ressources humaines ?
Les défis sont nombreux et nous obligent à disposer d'une bonne capacité d'anticipation. Cela s'explique par la très grande diversité du personnel – il existe près de quarante statuts au sein du SGDSN – et par leur rotation importante. Plusieurs dispositifs d'innovation sociale ont été déployés en 2015, dont un processus de reconversion interne des agents et le Pass – parcours d'accompagnement vers la suite du SGDSN – qui permet aux personnels en fin de contrat de retrouver un emploi. D'autres actions en faveur du personnel ont par ailleurs été lancées : l'accès au logement, l'apprentissage, l'emploi de personnels handicapés, la prévention des risques psychosociaux. Enfin, les actions de formation restent une priorité pour l'ensemble des agents.

En matière d'infrastructures, quels sont les principaux chantiers en cours ?
Je retiendrai les travaux de conduite de projet sur le futur centre informatique, l'aménagement d'une nouvelle salle de serveurs pour l'ANSSI ou encore la réalisation des travaux de rénovation sur le site de l'Hôtel national des Invalides, dans le cadre du plan HNI 2018.

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP
Tél. 01 71 75 80 00

www.sgdsn.gouv.fr