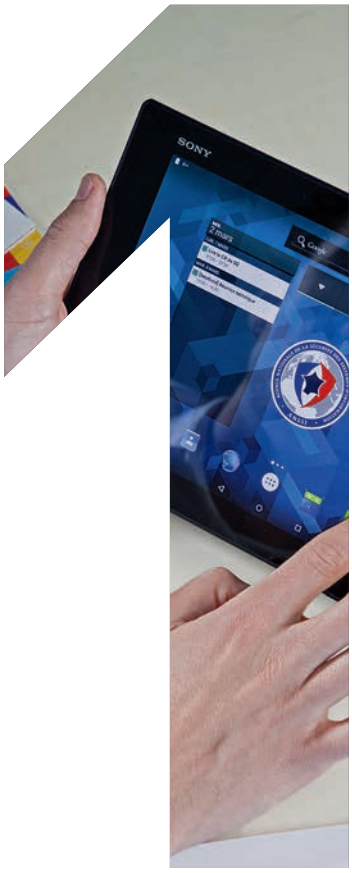
RAPPORT D'ACTIVITÉ

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN

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 : Scripto Sensu / Bertrand Vorimore
Crédits photos : couverture : MI›DICOM›F. PELLIER, MI›DICOMM›M.CEDE, ANSSI, MI›DICOM›J.ROCHA - p. 2 : Brian Wells Stevens - p. 4›7 : SGDSN - p. 8 : MI›DICOM›J.ROCHA - p. 9 : DR, MI›DICOM›E. DELELIS, DR, DR, DR, DR, DR, MI›DICOM›Y. MALENFER, DR, DR, MI›DICOMM›M.CEDE, DR - p. 10 : MI›DICOM› Y. MALENFER - p. 11 : MI›DICOM›P. CHABAUD, ECPAD/Défense›A. Karaghezian - MI›DICOM›J.GROISARD - p. 11›12 : ANSSI - p. 14 : MI›DICOM›J.ROCHA - p. 15 : Présidence de la République - p. 16›17 : MI›DICOM› F. PELLIER - p. 18 : MI›DICOM›Y. MALENFER - p. 19 : MI›DICOM›J.ROCHA - p. 20 : AFP Photo›J. Skarzynski - p. 21›25 : ANSSI - p. 26 : DR - p. 27 : iStock - p. 28›29 : One MBDA›D. Lutanie, ECPAD›S. LAFARGUE - p. 30 : DR - p. 31 : AFP Photo›J. Amiet, DR - p. 32 : MI›DICOM›J. ROCHA - p. 33 : MI›DICOM›Y. MALENFER - p. 34 : ECPAD/Défense›J. Faro - p. 35 : DR, MI›DICOM›J.ROCHA, DR - p. 36 : SGDSN - p. 37 : SGDSN - p. 39 : Brian Wells Stevens
Mai 2017

interview

LE SECRÉTAIRE GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

LOUIS GAUTIER
conseiller maître à la Cour des comptes, est secrétaire général de la défense et de la sécurité nationale depuis 2014.

> « Nous sommes entrés dans une gestion de crise au long cours. L'année 2016 marque la consolidation du modèle français de sécurité nationale. »

Comment qualifieriez-vous l'année 2016 ?

L'année 2015 avait été dominée par l'urgence, la crise, avec l'irruption brutale sur le territoire national du terrorisme islamiste, frappant d'abord en janvier, puis en novembre. Même si d'autres attentats sont survenus depuis, à Nice notamment, l'année 2016 marque la consolidation d'un nouveau modèle de protection de la population. Si, en 2015, nous avions été conduits à élaborer des réponses dans l'urgence, en 2016, nous avons gagné en expérience, nous avons adapté nos réponses opérationnelles : le dispositif Sentinelle – issu du contrat de protection des armées – a été dynamisé ; le plan VIGIPIRATE a été rénové en profondeur ; la coordination du renseignement a beaucoup progressé. Nous avons aussi travaillé à prévenir le danger potentiel représenté par les drones, avec le vote de la loi qui encadre ce nouvel usage. Nous envisageons désormais le terrorisme comme un problème au long cours.

Quel est votre rôle dans ce contexte ?

Le SGDSN est directement associé aux décisions prises par les plus hautes autorités de l'État en conseil de défense et de sécurité nationale (CDSN) : en amont des réunions hebdomadaires, il conduit les travaux de préparation des dossiers et, en aval, il assure le suivi des décisions. En assurant son secrétariat, il se trouve placé au cœur de l'instance de décision sur ces sujets cruciaux. Le SGDSN exerce une fonction d'animateur et de coordonnateur de l'action interministérielle dans ces domaines régaliens.

Le SGDSN constitue un modèle original…

C'est vrai. Un modèle particulier, bien adapté aux institutions de la Ve République, elles-mêmes spécifiques. Son originalité repose sur la double nature de sa mission – à la fois secrétariat général et opérateur de sécurité – et sur le fait qu'il est « serviteur de deux maîtres », à savoir le Président de la République et le Premier ministre. Ce positionnement, qui s'incarne dans son rôle au conseil de défense et de sécurité nationale, s'avère particulièrement judicieux. Le SGDSN assure une fonction de cohérence entre l'Élysée et Matignon. Aujourd'hui, l'idée de « sécurité nationale », qui complète depuis 2009 l'intitulé SGDN, a pris toute sa signification : depuis 2015, le SGDSN a fait la démonstration de sa capacité à animer le travail interministériel et la conduite de la gestion de crise. Une autre de ses spécificités concerne son inscription dans la durée. Nous sommes en anticipation réactive dans la gestion de la crise et, en même temps, nous assurons une mission de continuité pour l'État.

Ce modèle subit-il des évolutions ?

Il s'adapte en permanence. L'une de nos forces vient de notre expertise sur des sujets de pointe. Ce modèle, très évolutif, se reforge dans l'émergence de nouvelles problématiques au fil des ans. Cette capacité d'adaptation s'appuie sur des équipes aux compétences diversifiées : des diplomates, des policiers, des militaires, bien sûr, mais aussi des ingénieurs, des scientifiques, etc. Tous sont d'authentiques spécialistes de leur domaine et de son ingénierie de sécurité. Cela offre une grande richesse par le croisement de points de vue très différents.

Un événement marquant en 2016 : Eurofoot…

Nous étions scrutés par le monde entier, avec des millions de visiteurs et la problématique nouvelle des « fan zones » à prendre en compte. L'efficacité du plan VIGIPIRATE a été démontrée, tout comme sa grande capacité d'adaptation. Plus globalement, nous avons renforcé notre réactivité grâce à des plans multidimensionnels intégrant de mieux en mieux la problématique cybernétique. Nous avons aussi beaucoup travaillé à la sensibilisation de la population, au travers de la campagne « *Comment réagir en cas d'attaque terroriste ?* ».

Quel rôle le SGDSN joue-t-il au plan international ?

Nous assumons la coordination de plusieurs stratégies interministérielles et portons la position française auprès des institutions internationales. C'est le cas, notamment, pour le système de géopositionnement par satellites « Galileo », en service depuis décembre 2016. Ce dispositif va garantir à l'Europe la sécurité de ses communications civiles et militaires. C'est le cas également en matière de cybersécurité : la France mobilise ses partenaires européens autour de la cybermenace, sujet sur lequel la prise de conscience n'est pas encore partagée par tous. Or il ne peut y avoir de véritable cybersécurité qu'à la dimension européenne. La France est à la pointe sur ce sujet grâce aux compétences et à l'action de l'ANSSI. Ce sujet de la cybersécurité constitue un enjeu fort : aujourd'hui, on ne peut plus envisager une menace sans prendre en compte sa dimension numérique.

Quelles sont vos priorités pour 2017 ?

Finalisation d'un rapport de prospective, organisation de la première conférence internationale « Construire la paix et la sécurité de la société numérique », réforme de la réglementation du secret de la défense nationale, etc. les chantiers sont nombreux. Nous devons aussi prolonger la croissance de l'ANSSI. Et nous aurons un rôle important pour assurer la continuité de l'État, à l'occasion des renouvellements qui interviendront en son sein à l'issue des échéances électorales.

LE SGDSN EN UN COUP D'ŒIL

Placé au cœur de l'exécutif, le SGDSN assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Il assure le secrétariat des conseils de défense et de sécurité nationale que préside le chef de l'État. 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 les domaines 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 assure trois missions principales :

La veille et l'alerte face aux menaces et aux risques.
1 Dans ce cadre, le SGDSN est chargé du suivi des crises, de la préparation des plans gouvernementaux et de l'organisation de l'État en temps de crise.

Le conseil et la rédaction des décisions prises par l'exécutif en matière
2 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.

Le rôle d'opérateur de sécurité nationale, dans la gestion des
3 habilitations, des documents classifiés, des communications gouvernementales – à travers la gestion du centre de transmissions gouvernemental (CTG) – ou encore de la cyberdéfense, *via* l'Agence nationale de la sécurité des systèmes d'information (ANSSI), rattachée au SGDSN.

QUI ?

972

agents répartis au sein du SGDSN, de l'ANSSI, du CTG et du GIC.

COMBIEN ?

276,2

millions d'euros de budget en loi de finances initiale pour 2017.

OÙ ?

Invalides

Le SGDSN est installé dans une partie des locaux de l'hôtel national des Invalides, à Paris.

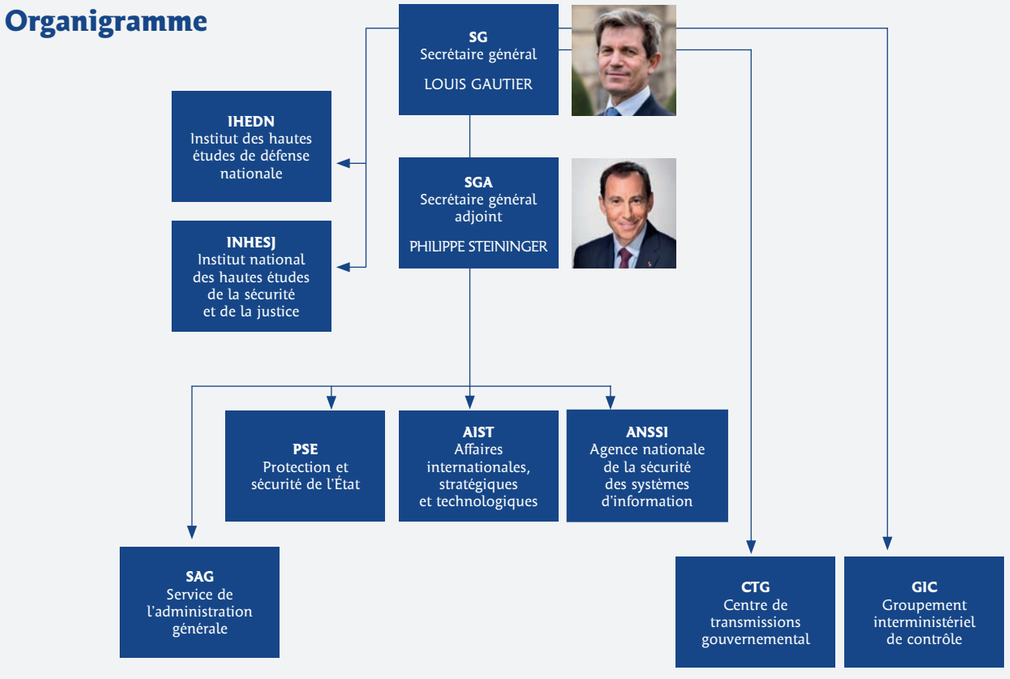
12 DOMAINES D'INTERVENTION

- **Assurer** le secrétariat du conseil de défense et de sécurité nationale
- **Réagir** en cas de crise
- **Lutter** contre la prolifération
- **Anticiper** les risques et les menaces
- **Protéger** le potentiel scientifique et technique de la Nation
- **Assurer** la cyberdéfense
- **Améliorer** les dispositifs de prévention et de protection
- **Contrôler** les exportations de matériel de guerre
- **Protéger** le secret de la défense et de la sécurité nationale
- **Préparer** la réponse aux crises
- **Suivre** les questions de sécurité internationale
- **Sécuriser** les programmes spatiaux européens

DE SGDN À SGDSN

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. Un choix stratégique validé par la réalité des menaces affrontées depuis 2015 par le pays.

Organigramme



LE SGDSN EN 2016

17 février
Remise au Premier ministre du rapport sur la dynamisation du dispositif Sentinelle

7 mars
Début de l'exercice « Crues de Seine » organisé par le SGDSN

22 mars
Lancement de la campagne nationale *« Comment réagir en cas d'attaque terroriste ? »*

3 mai
Remise au Premier ministre du rapport sur la sécurité des sites « Seveso »

13 juin
Double meurtre à Magnanville (Yvelines)

14 juillet
Attentat sur la promenade des Anglais à Nice

26 juillet
Attentat à l'église de Saint-Étienne-du-Rouvray (Seine-Maritime)

20 septembre
Premières Assises de la filière des industries de sécurité

22 octobre
Approbation par le Premier ministre de la stratégie nationale de sûreté des espaces maritimes

24 octobre
Promulgation de la loi sur les drones civils

30 novembre
Publication du nouveau plan VIGIPIRATE

22 décembre
Colloque « Le SGDSN, 110 ans au service de la défense et de la sécurité » à la Maison de la Chimie

EUROFOOT 2016

Plusieurs millions de supporters venus de l'Europe entière, une dizaine de villes hôtes réparties dans tout l'Hexagone, 51 matchs durant un mois de compétition… Pour la première fois, l'Eurofoot réunissait 24 équipes nationales, attirant des visiteurs venant de chacun de ces pays. Dans un contexte de menace terroriste et d'état d'urgence, organiser le championnat d'Europe de football du 10 juin au 10 juillet 2016 représentait pour la France un défi majeur en termes de sécurité.

10
villes mobilisées
Dix grandes villes ont accueilli les matchs du championnat d'Europe : Bordeaux, Lens, Lille, Lyon, Marseille, Nice, Paris, Saint-Denis, Saint-Étienne et Toulouse.

1
mois sous tension
Entamé par le match d'ouverture le 10 juin, l'Eurofoot s'étirait sur un mois complet, jusqu'à la finale entre le Portugal et la France le 10 juillet, à Saint-Denis.

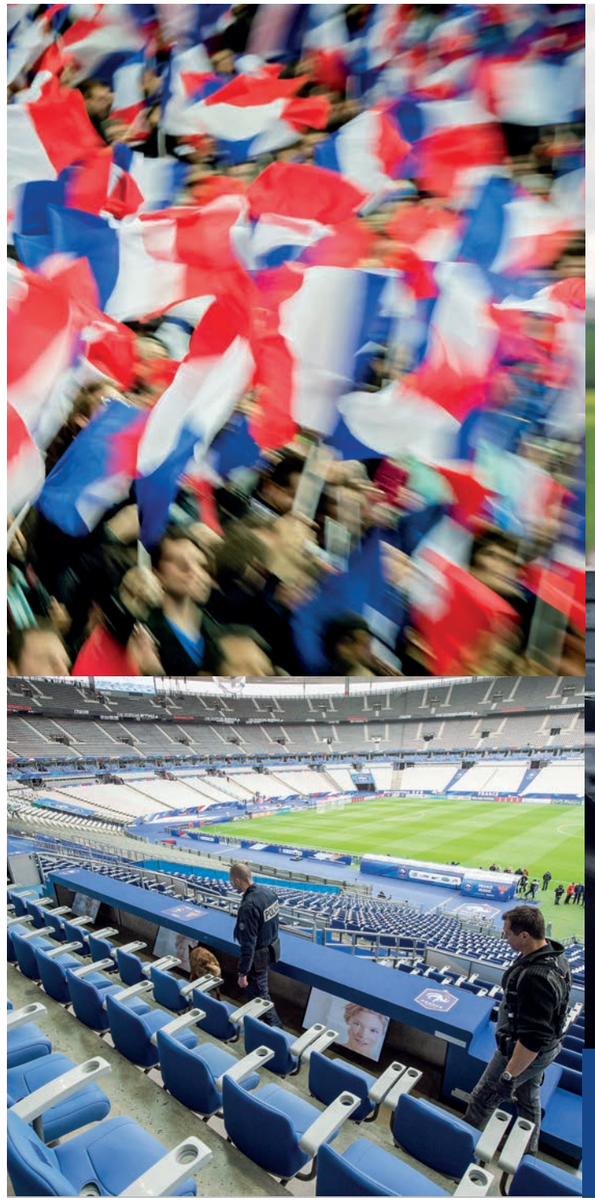
2 500 000
supporters
Au total, les 51 matchs de la compétition ont attiré 2 500 000 spectateurs dans les stades des villes hôtes, sans compter ceux qui se sont massés dans les « fan zones ».

FAN ZONES / L'édition 2016 marquait l'introduction d'une grande nouveauté pour un événement sportif organisé dans l'Hexagone : la mise en place de « fan zones » au cœur des villes, des périmètres réservés aux spectateurs leur permettant de suivre les matchs sur écran géant dans une ambiance festive. Un dispositif recommandé par l'union européenne de football (UEFA) pour éviter des rassemblements diffus, plus difficiles à sécuriser. Mais cette concentration de spectateurs dans les « fan zones » imposait des mesures de sécurité renforcées à leurs points d'accès. Plusieurs millions de spectateurs venus de l'Europe et du monde entier s'y sont rendus, sans incident majeur.

COPRODUCTION / Cet événement d'une ampleur exceptionnelle s'est déroulé dans un contexte particulier, marqué par la menace terroriste, et sous les yeux de millions de téléspectateurs du monde entier. La compétition a bénéficié à ce titre d'un niveau de sécurité tout à fait exceptionnel, résultat d'une véritable coproduction entre l'État, les organisateurs et les villes hôtes. Le SGDSN a participé étroitement à la préparation de l'Eurofoot, en particulier dans deux domaines relevant de sa compétence : la préparation à la gestion d'une crise majeure et le plan VIGIPIRATE.

PRÉPARATION / Le SGDSN a coordonné les travaux de préparation à une crise majeure en mettant en place un plan d'action spécifique, en lien avec la direction générale de la sécurité civile et de la gestion de crise (DGSCGC) du ministère de l'intérieur. Pour tester l'articulation des responsabilités et des dispositifs de crise des différents acteurs impliqués dans l'événement – État, organisateur, collectivités territoriales –, il a piloté l'organisation, en octobre 2015, d'un exercice gouvernemental, EUROFOOT15, véritable répétition de l'événement. Le SGDSN a, en particulier, animé la réflexion sur les mesures à prendre en cas d'attaque non conventionnelle.

VIGIPIRATE / La posture VIGIPIRATE adoptée pour l'Eurofoot 2016 a fait l'objet d'une démarche interministérielle approfondie pour adapter les mesures aux spécificités de la compétition. L'accent a ainsi été mis sur la protection des sites concernés : les stades, les fan zones, les lieux de résidence et les centres d'entraînement des équipes nationales. Étaient notamment intégrés à cette démarche la prise en compte de la menace « nucléaire-radiologique-bactériologique-chimique-explosif » (NRBC-E), le cyber-risque et la nécessaire protection de l'espace aérien, notamment contre l'utilisation malveillante de drones.
Fortement impliqué dans le pilotage de la sécurité tout au long de l'Eurofoot, le SGDSN assurait la coordination des moyens de sécurité dans le cadre de la cellule interministérielle de crise (CIC), réunie chaque soir pendant un mois. Le 10 juillet, la compétition s'est clôturée sans qu'aucun incident marquant, de nature terroriste, n'ait affecté le bon déroulement de la compétition.



Un rendez-vous à hauts risques

temps fort

PIRANET 16

Premier exercice majeur de cyberattaque

Le *Livre blanc sur la défense et la sécurité nationale* de 2013 insiste sur la nécessité, pour l'État, de renforcer ses capacités de gestion des crises majeures. Dans cette logique, le SGDSN est chargé de mettre en œuvre une politique de professionnalisation des acteurs de la gestion de crise. Parmi les moyens de cette politique figure l'organisation, chaque année, de trois exercices gouvernementaux.

PREMIÈRE / En 2016, le SGDSN pilotait le premier exercice majeur de réponse à une attaque sur les systèmes d'information mettant en jeu le fonctionnement même de l'État. Joué du 6 au 8 décembre 2016, l'exercice PIRANET 16 s'est déroulé dans un contexte totalement rénové par rapport à sa précédente édition, datant de 2012 : une nouvelle organisation gouvernementale de gestion des crises majeures, instituée par la circulaire du 2 janvier 2012 et centrée sur la cellule interministérielle de crise (CIC) ; une montée en puissance significative de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ; l'existence d'un nouveau plan gouvernemental d'intervention en cas d'atteinte majeure à la continuité des systèmes d'information liés aux activités vitales de la Nation (plan PIRANET).

SCÉNARIO / Simulant une crise grave consécutive à une série de cyberattaques de grande ampleur d'origine étatique étrangère contre un ministère et un opérateur majeur du secteur de l'énergie, le scénario prévoyait des effets sur l'ensemble des services de l'État. PIRANET mettait en présence 170 intervenants mobilisés sur trois jours, autour de trois objectifs : mettre en œuvre le projet de plan PIRANET pour vérifier sa validité avant son adoption ; préparer les décisions stratégiques relevant du niveau politique et organiser la communication de crise face à une cyberattaque majeure. La direction de la protection et de la sécurité de l'État (PSE) et l'Agence nationale de sécurité des systèmes d'information (ANSSI) ont préalablement réuni l'ensemble des acteurs afin de recueillir leurs attentes et de recenser leurs besoins.

ACTEURS / Placées au cœur de l'exercice, les équipes de l'ANSSI ont élaboré le scénario technique, co-animé l'exercice avec la direction de la PSE et piloté la gestion de la crise en relation étroite avec le ministère de l'intérieur et le ministère de l'environnement, de l'énergie et de la mer, notamment. La cellule interministérielle de crise, activée sur décision du Premier ministre, était dirigée par Guillaume Poupard, directeur général de l'ANSSI, et a mobilisé 90 agents.

VALIDITÉ / Riche d'enseignements, l'exercice a montré la pertinence du projet de plan, le bon niveau des travaux de la cellule interministérielle de crise et une capacité à communiquer sur une situation de crise aux caractéristiques très spécifiques. Il a aussi souligné la nécessité de poursuivre les efforts en matière de développement des capacités de cyberdéfense de l'ensemble des acteurs. PIRANET est un plan gouvernemental de la famille PIRATE, qui regroupe les plans d'interventions complémentaires à VIGIPIRATE, centrés chacun sur une thématique et une menace spécifique. C'est l'un des piliers de la stratégie de défense informatique française. La mise à jour de ce catalogue de plans est un effort permanent pour le SGDSN, qui s'attache à les rénover un à un en publiant des plans de nouvelle génération, toujours plus directement opérationnels en cas de crise.

ENSEIGNEMENTS / L'exercice a permis de mettre en lumière le caractère indispensable des réseaux d'information étatiques dans la gestion d'une crise importante et la continuité des services de l'État. Ce caractère indispensable justifie un effort tout particulier de préservation face à de potentielles cyberattaques. Il a aussi permis de valider une stratégie générale de réponse à la crise articulée autour de quatre axes à définir en priorité : l'objectif à atteindre en sortie de crise ; les contraintes majeures qui pèsent sur l'action ; la stratégie en matière de relations internationales et la communication gouvernementale.

170

AGENTS SUR LE PONT

Au total, près de 170 personnes, dans les différents services impliqués, ont participé à l'exercice de cyberdéfense PIRANET 16, en décembre 2016.

Le plan

PIRANET

Ce plan gouvernemental d'intervention est l'un des piliers de la défense française en matière de systèmes d'information.

2016

LES NOUVEAUTÉS

Le jeu de la cellule interministérielle de crise, le rôle central de l'ANSSI et le support constitué par le plan PIRANET.

COORDONNER et PILOTER

Le secrétariat général de la défense et de la sécurité nationale (SGDSN) est placé auprès du Premier ministre et travaille en relation étroite avec la présidence de la République. Au cœur de l'exécutif, il contribue à l'exercice du pouvoir régalien en matière de sécurité nationale et participe à l'organisation de la réponse aux crises auxquelles les pouvoirs publics sont confrontés. Son intervention s'étend des conseils de défense et de sécurité nationale, dont il assume le secrétariat, à l'animation des travaux interministériels sur des sujets aussi différents que le suivi des crises internationales ou la structuration d'une filière industrielle de la sécurité.

CDSN. Le SGDSN assure le secrétariat du CDSN, dont il organise les travaux préparatoires et le suivi des décisions.

Le SGDSN est chargé de la conduite des actions interministérielles concourant à cette stratégie de défense et de sécurité nationale de la France, telle qu'elle a été exposée dans le *Livre Blanc sur la défense et la sécurité nationale* du 24 avril 2013, avec l'objectif de limiter les conséquences d'une crise majeure sur la vie du pays et de faciliter le retour à une situation normale. Dans ce cadre, il anime les travaux interministériels sur l'analyse des risques et des menaces, l'organisation de l'État face aux crises majeures, la planification gouvernementale en matière de sécurité, 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 et la protection du secret de la défense nationale.

Le CDSN, centre du dispositif de sécurité nationale

Le SGDSN assume le secrétariat des conseils de défense et de sécurité nationale (CDSN). Au sommet de l'État, cette instance concentre l'autorité en matière de pilotage général de la défense et de direction politique et stratégique de la réponse aux crises majeures. Présidé par le chef de l'État en présence du Premier ministre, le CDSN est compétent pour toutes les questions de défense et de sécurité, qu'il s'agisse de la programmation militaire, de la politique de dissuasion, de la lutte contre le terrorisme, de la sécurité économique et énergétique ou de la planification de la réponse aux crises.

Rassemblant les ministres de la défense, de l'intérieur, de l'économie, du budget et des affaires étrangères, ouvert à d'autres membres du Gouvernement si le Président le juge nécessaire, le CDSN peut se réunir en formation restreinte, par exemple pour la conduite d'opérations extérieures. Il traite des sujets spécifiques en formations spécialisées : en conseil national du renseignement, il arrête les orientations, les priorités stratégiques et les moyens des services spécialisés ; en conseil des armements nucléaires, il règle l'ensemble des questions relatives à la dissuasion (doctrine, format des forces, programmes…).

Le secrétariat du conseil constitue la mission historique du secrétaire général de la défense et de la sécurité nationale, qui l'assume depuis plus d'un siècle sous des dénominations variées. Depuis 2009, afin d'assurer la totale cohérence des décisions prises et du suivi de leur mise en œuvre, le CDSN examine l'ensemble des questions relevant du champ de la défense et de la sécurité nationale (programmation militaire,

Un CDSN par semaine

Le conseil de défense et de sécurité nationale, dont le SGDSN assure le secrétariat, s'est réuni à 32 reprises en 2016. À compter du 14 juillet 2016, ses réunions sont devenues hebdomadaires.

GESTION DE CRISE. Le SGDSN participe directement à la gestion des crises au sein de la CIC.

36
jours de crise

Le SGDSN participe à la cellule interministérielle de crise, activée 36 jours en 2016. Habituellement, elle est activée entre 6 et 10 jours par an, pour des exercices.

opérations extérieures, renseignement, sécurité intérieure…). Conformément aux directives du Président de la République et du Premier ministre, le secrétaire général conduit, en liaison avec les ministères concernés, les travaux préparatoires aux réunions du CDSN, dont il établit les relevés de décision, notifiant ensuite les décisions prises et s'assurant de leur exécution par les services de l'État.

Alimenter en information et appuyer la décision

Par son rôle auprès des plus hautes autorités de l'État, le SGDSN se trouve au cœur du dispositif de sécurité nationale et de lutte contre le terrorisme : face à la menace permanente et en situation d'état d'urgence, le conseil de défense et de sécurité nationale a pris une dimension nouvelle. Il est l'instance de décision de la politique de sécurité nationale. Convoqué à dix reprises en 2015 par le Président de la République, le rythme de ses réunions s'est progressivement accéléré. À compter de l'attentat de Nice, le 14 juillet 2016, le CDSN s'est réuni de manière hebdomadaire.

Avant chacune de ces réunions, le SGDSN effectue, en liaison avec les différents services spécialisés, un travail de synthèse du renseignement pour alimenter les travaux du conseil. Sa direction des affaires internationales, stratégiques et technologiques (AIST) apporte un appui permanent au coordonnateur national du renseignement, pour lequel elle assure l'animation de groupes de travail, leur secrétariat et la synthèse des informations recueillies par les services spécialisés sur la menace terroriste contre le territoire national, l'activité des États « proliférants » et « proliférateurs » en matière nucléaire, chimique ou biologique, les trafics d'armes, etc.

Cellule interministérielle de crise : au cœur de la gestion de crise

Attentats de Bruxelles en mars, double meurtre à Magnanville le 13 juin, attentats de Nice le 14 juillet, assassinat de Saint-Étienne-du-Rouvray le 26 juillet… L'année 2016 a été jalonnée de crises ayant nécessité une réaction rapide et globale de l'État. L'organisation de cette réponse est la fonction de la cellule interministérielle de crise (CIC), activée sur décision du Premier ministre. Armée 36 jours en 2016, la CIC regroupe en moins d'une heure représentants des ministères, experts et opérateurs, sous la direction d'une autorité désignée par le Premier ministre. Au sein de la CIC, la cellule « Situation » dresse un état des lieux et les conséquences potentielles de la crise ; la cellule « Anticipation » identifie les événements risquant de compliquer la gestion de la situation ; la cellule « Décision » prépare les décisions des autorités ; la cellule « Communication », enfin, est chargée de l'information de la population.

Partie prenante à la CIC, le SGDSN est directement associé à la gestion de la crise, via sa direction de la protection et de la sécurité de l'État (PSE), qui élabore des solutions et des mesures concrètes…

Objectif : être en mesure de proposer rapidement, quelle que soit la nature de la crise, des solutions préparées à l'avance que les préfets peuvent mettre en œuvre. C'est la raison d'être des plans et des exercices conçus par le SGDSN. Dans cette logique d'anticipation, chaque sortie de crise est l'occasion d'un retour d'expérience afin d'améliorer les pratiques et de promouvoir la culture de l'anticipation des risques et de gestion des crises.

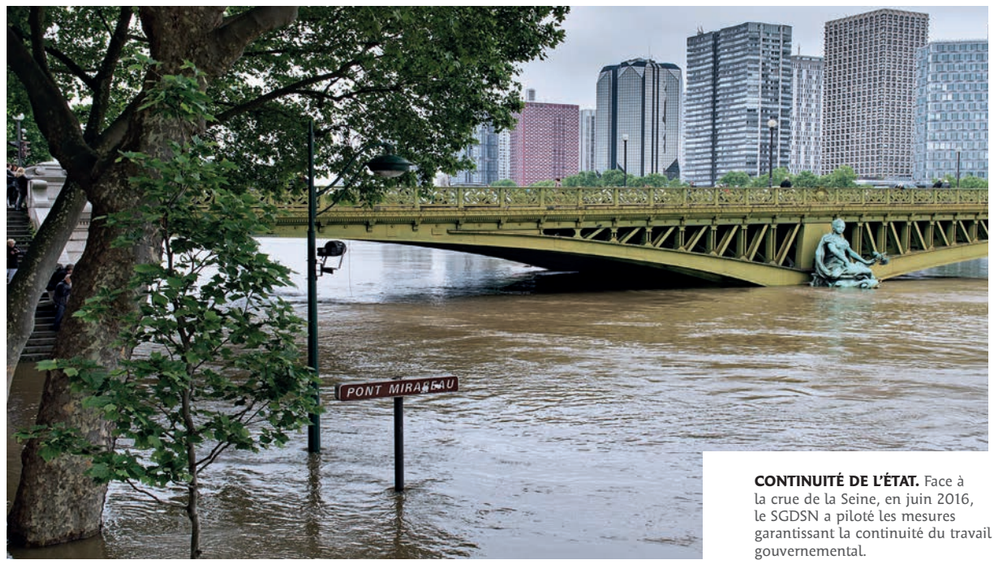
Plan d'action contre la radicalisation et le terrorisme

A l'occasion du comité interministériel pour la prévention de la délinquance et de la radicalisation (CIPDR) du 9 mai 2016, le Premier ministre a validé le nouveau plan d'action contre la radicalisation et le terrorisme (PART). Parmi les 80 mesures qui composent ce plan, trois ont été plus particulièrement suivies en 2016 par le SGDSN :

➔ le renforcement du dispositif des enquêtes de criblage des personnels aéroportuaires, avec la publication de l'arrêté du 16 septembre 2016 portant autorisation d'un système de traitement informatisé des titres de circulation et des habilitations (STITCH) et le lancement d'une expérimentation sur le site pilote de Toulouse pour tester un portail de dépôt de demandes dématérialisées ;
➔ le renforcement de la sécurité des plateformes aéroportuaires et des transports ferroviaires, notamment des grandes gares et interconnexions, avec en particulier un appel d'offres dans le cadre du deuxième programme des Investissement d'avenir lancé en octobre 2016 ;
➔ le renforcement de la protection des sites nucléaires civils, avec la création du commandement spécialisé pour la sécurité du nucléaire (CoSSeN), placé au sein de la gendarmerie nationale. Le SGDSN a plus particulièrement assuré la coordination interministérielle pour la détermination des missions du CoSSeN, qui pourrait être opérationnel à l'été 2017.

Crue de la Seine et Eurofoot

Au-delà de la gestion des attentats et de leurs suites, deux événements majeurs ont marqué l'année 2016 et nécessité la mise en œuvre d'un véritable dispositif de gestion de crise : la crue de la Seine, du 1er au 7 juin, et l'Euro de football, du 10 juin au 10 juillet. Début juin 2016, la Seine enregistrait un pic de crue à 6,10 mètres, un niveau qu'elle n'avait pas atteint depuis près de trente ans. Très vite, les voies sur berges étaient inondées, le RER C, le musée



CONTINUITÉ DE L'ÉTAT. Face à la crue de la Seine, en juin 2016, le SGDSN a piloté les mesures garantissant la continuité du travail gouvernemental.

SOUS SURVEILLANCE. Face à la menace terroriste, l'Eurofoot 2016 a nécessité le déploiement d'un important dispositif de sécurité, piloté par le SGDSN et l'intérieur.

d'Orsay, le Louvre et le Grand Palais contraints de fermer leurs portes, etc. La proximité de certains ministères avec la Seine pouvait faire craindre des dysfonctionnements importants. La situation a nécessité la mise en œuvre de mesures de précaution et de résilience par le SGDSN pour garantir la continuité du travail gouvernemental. L'exercice joué deux mois plus tôt *(lire plus loin)* a, à cet égard, constitué un atout important pour faire face à la crue et limiter ses conséquences sur le fonctionnement de l'appareil d'État.

3
exercices majeurs en un an

Sécurité nucléaire, risque cybernétique, aléas climatiques… les exercices gouvernementaux organisés en 2016 contribuent à améliorer la planification de la réponse aux menaces.

L'organisation du championnat d'Europe de football par la France présentait, elle, un risque d'une toute autre nature, en raison de la menace terroriste. La durée de l'événement (un mois), sa couverture nationale (10 villes hôtes) et la nouveauté que représentait l'organisation de « fan zones » ont justifié la mise en place d'un dispositif global de sécurité auquel le SGDSN a été étroitement associé, en coordination avec le ministère de l'intérieur *(lire « temps fort » en page 10)*.

En 2016, trois exercices de préparation aux crises

Responsable de la préparation et de la mise en œuvre des mesures de défense et de sécurité dont le Premier ministre a la responsabilité en cas de crise majeure, le SGDSN pilote, pour le compte de celui-ci, les exercices gouvernementaux relevant de la planification de sécurité nationale. Trois exercices ont été joués en 2016 : « Crues de Seine », « SECNUC 16 » et « PIRANET 16 ».

En mars, l'exercice « Crues de Seine » a permis de vérifier la capacité de la cellule interministérielle de crise et des administrations centrales à réagir à une submersion partielle de la capitale et à assurer le déménagement en urgence des directions et services de plusieurs ministères vers des installations de repli. Articulé avec l'exercice « EU SEQUANA 16 », organisé, lui, par la zone de défense et de sécurité de Paris, il été l'occasion de tester le plan de continuité du travail gouvernemental dans le cas d'une crue majeure du fleuve. La cellule interministérielle de crise, armée et chargée de la gestion opérationnelle de la crise, a, elle-même, déménagé de la place Beauvau vers son site de repli. Cet exercice a eu une application quasi immédiate : début juin, la Seine entrait réellement en crue et le Premier ministre, sur proposition du SGDSN et après avis du ministère de l'intérieur, décidait de mettre en œuvre le plan de continuité du travail gouvernemental et activait une série de mesures de vigilance et d'alerte. Les enseignements tirés de l'exercice de mars et de la crue de juin permettront d'apporter pour l'avenir des améliorations au plan existant, en coordination avec l'ensemble des ministères, représentés par leurs hauts fonctionnaires de défense et de sécurité nationale.

En septembre, l'exercice « SECNUC 16 » mettait en scène un scénario de catastrophe industrielle nucléaire. Centré sur un site localisé dans le département de la Manche, l'exercice a mobilisé la préfecture de Saint-Lô pendant deux jours et fait jouer de nombreux organismes : la cellule interministérielle de crise, qui a piloté la réponse à la crise ; le préfet de département, maître d'œuvre sur le terrain ; mais aussi l'Autorité de sûreté nucléaire (ASN) et l'Institut de radioprotection et de sûreté nucléaire (IRSN). Au total, plusieurs dizaines de personnes ont participé à ce « jeu » qui met en présence deux parties : l'organisateur, qui construit un scénario et qui « injecte » des événements, et les joueurs, qui construisent des réponses, sous le contrôle d'arbitres. Ce type d'exercice se prolonge ensuite par un double retour d'expérience : le premier, fait « à chaud », suivi d'un second, organisé six semaines plus tard pour bénéficier de plus de recul.

En décembre, « PIRANET 16 » constituait le premier exercice majeur de cyberattaque contre les systèmes d'information, mettant en cause le fonctionnement même de l'État *(lire « temps fort » en page 12)*. Organisé selon un scénario original, cet exercice associait le ministère de l'intérieur, les ministères chargés de l'énergie et des transports, mais aussi le SGDSN, par l'intermédiaire notamment des équipes de l'Agence nationale de sécurité des systèmes d'information (ANSSI), directement associée pour l'occasion à la cellule interministérielle de crise. Riche d'enseignements, cet exercice a montré la capacité de la France à construire une réponse globale au risque cybernétique. Les conclusions qui ont été tirées contribueront à la mise à jour du plan PIRANET *(lire « Éclairer et Planifier » en page 32)*.

CGI
1re année de mise en œuvre

Le Contrat général interministériel organise la planification capacitaire de la contribution des ministères civils à la gestion des crises pour la période 2015-2019.

L'instruction générale interministérielle signée en février 2015 par le Premier ministre définit un Contrat général interministériel (CGI) pour la période 2015-2019. Ce contrat fixe les capacités exigibles des ministères civils et leur niveau d'engagement, en complément des autres acteurs de la gestion des crises : armées, collectivités territoriales, opérateurs d'importance vitale. Résultat d'un travail interministériel mené pendant deux ans sous l'égide du SGDSN, le CGI s'enrichit des retours d'expérience tirés des crises terroristes et de la préparation de l'Eurofoot 2016.

En 2016, le SGDSN a notamment financé, pour le compte du ministère des affaires sociales et de la santé, l'achat d'équipements de protection NRBC (nucléaire-radiologique-bactériologique-chimique) destinés aux Samu et a tenu une réunion interministérielle pour analyser les engagements financiers déjà réalisés par les ministères et ceux qui sont envisagés pour 2017. Cette démarche de Contrat général interministériel a permis de mieux appréhender l'évaluation de la menace dans le dispositif du nouveau plan VIGIPIRATE et de bien identifier les capacités essentielles à la résilience de la Nation. Le SGDSN y contribue largement par les analyses thématiques régulières qu'il met à la disposition du Gouvernement.

Le CTG, administrateur des transmissions sécurisées

Placé sous l'autorité du SGDSN, le centre de transmissions gouvernemental (CTG) garantit la permanence des moyens de communication au profit du Président de la République et du Premier ministre. Cette unité militaire interarmées de près de 200 hommes et femmes est installée aux Invalides et s'appuie sur trois détachements : deux stationnés à l'Élysée, un à l'hôtel Matignon.

SES MISSIONS

- ➔ Mettre en œuvre les transmissions sécurisées du Président de la République et du Premier ministre.
- ➔ Diffuser 24 h/24 à l'état-major du Président et au cabinet militaire du Premier ministre les informations reçues sur les réseaux sécurisés.
- ➔ Administrer les moyens interministériels de transmission sécurisés contribuant à la gestion de crise.
- ➔ Assurer l'exploitation des systèmes d'information gouvernementaux sécurisés (messagerie interministérielle ISIS, système de téléphonie de niveau secret défense TEOREM…).

Le Contrat général interministériel, pour organiser les capacités civiles

Face aux risques et aux menaces qui peuvent affecter le pays, l'État doit pouvoir compter sur toutes les capacités – civiles et militaires– dont il dispose. D'où la nécessité de les organiser de manière à les mettre en œuvre, le cas échéant.

Anticiper les crises internationales à venir

Le retour à des rapports de puissance à puissance (États-Unis, Chine, Russie), les incertitudes liées au *Brexit* et aux élections américaines, la montée des périls dans plusieurs régions du monde sont autant de sujets qui mobilisent les équipes de la direction des affaires internationales, stratégiques et technologiques (AIST) du SGDSN. Le SGDSN assume en effet un rôle actif de veille, de synthèse, d'alerte et d'appui à la décision sur les questions de sécurité internationale, au profit de la présidence de la République et du cabinet du Premier ministre, dans le cadre de mandats *ad hoc*.

Pour ce faire, il s'appuie notamment sur le partenariat développé avec des organismes de recherche stratégique reconnus pour la pertinence de leurs analyses prospectives et la richesse de leurs études sur les questions de défense et de sécurité. Le SGDSN anime un groupe interministériel d'anticipation des crises, qui traite de pays où une crise est possible et où la France a des intérêts importants. Le groupe a pour mission de dresser des scénarios d'évolution et des recommandations articulant prévention et réaction. Le SGDSN peut aussi être sollicité pour mettre en place des groupes interministériels de travail consacrés à certains théâtres d'opérations ou à une crise internationale. Le SGDSN pilote notamment la « stratégie interministérielle sahélo-saharienne », qui vise à renforcer les capacités de souveraineté et de gouvernance des pays de la zone concernée. Cette stratégie a fait l'objet d'une importante mise à jour au printemps 2016.

INTERMINISTÉRIEL. Le SGDSN pilote l'élaboration de la position française sur la défense anti-missiles balistiques, portée par le chef de l'État au sommet de l'OTAN à Varsovie.

Pilotage de stratégies interministérielles ciblées

Dans le cadre de sa mission de veille et d'alerte des autorités (Président de la République et Premier ministre), le SGDSN pilote des groupes de travail interministériels sur des thèmes intéressant la sécurité nationale ou internationale, comme la dissémination des armements légers et de petits calibres, la piraterie maritime ou le suivi de l'accord sur les activités nucléaires iraniennes. Le SGDSN, représenté par sa direction AIST, est chargé de coordonner la réflexion interministérielle afin de proposer au Président de la République et au Premier ministre des orientations et des moyens susceptibles d'assurer ou de renforcer la sécurité nationale. C'est le cas notamment sur le sujet de la défense anti-missiles balistiques (DAMB), pour lequel elle a assuré la coordination interministérielle afin de fixer la position française défendue lors du sommet de l'OTAN qui s'est tenu à Varsovie les 8 et 9 juillet 2016.

La montée en puissance d'une filière industrielle de la sécurité

La sécurisation des espaces publics, des transports, des bâtiments officiels ainsi que des opérateurs d'importance vitale impose à l'État de disposer de partenaires industriels capables de lui apporter, rapidement et au meilleur coût, les solutions dont il a besoin. C'est le sens de la démarche de structuration de la filière nationale des industries de sécurité, animée par le SGDSN en application des recommandations du *Livre blanc sur la défense et la sécurité nationale* de 2013. Installé le 23 octobre 2013, le comité de la filière industrielle de sécurité (CoFIS) s'attache à promouvoir la compétitivité d'une filière dont le marché est évalué, à l'échelle nationale, à 30 milliards d'euros et 300 000 emplois. Le comité associe industriels, institutionnels, opérateurs – utilisateurs de ces technologies – et experts.

LES CHAMPS DE LA SÉCURITÉ. Le SGDSN travaille à la structuration de la filière industrielle de sécurité

Cette démarche, qui s'articule avec les plans de la « Nouvelle France industrielle » et la stratégie nationale de recherche, bénéficie des fonds du programme des Investissements d'avenir. Des projets pilotes ont été lancés dans les domaines des radiotélécommunications mobiles pour les forces de sécurité, des plateformes de vidéoprotection ou de la lutte contre l'utilisation malveillante des drones, en particulier. L'année 2016 a été, pour le CoFIS, consacrée à la mise en œuvre de la feuille de route validée le 1er décembre 2015 sous la co-présidence des ministres de l'économie et de l'intérieur. Avec un temps fort : la tenue à Paris, le 20 septembre, des premières Assises de la filière des industries de sécurité, qui ont réuni plus de 300 entreprises de toutes tailles, engagées dans la construction d'une offre nouvelle, indispensable à l'avenir.

Coordonner et Piloter | Protéger et Sécuriser | Contrôler et Certifier | Éclairer et Planifier

PROTÉGER et SÉCURISER

L'omniprésence des technologies numériques dans tous les aspects de la vie du pays l'expose à de nouvelles menaces dans le domaine cybernétique. Pour faire face à ces risques, la France s'est dotée d'une stratégie nationale pour la sécurité du numérique, dont la mise en œuvre est confiée à l'Agence nationale de la sécurité des systèmes d'information (ANSSI), au sein du SGDSN. L'enjeu est de taille : garantir la souveraineté nationale en sécurisant les systèmes d'information de l'État et instaurer la confiance numérique, préalable nécessaire au développement de cette nouvelle économie.

CYBERDÉFENSE. Par son rattachement au SGDSN, l'ANSSI s'incrit dans la chaîne de la défense et de la sécurité nationale

Un modèle original, interministériel et centré sur la défense

Le secrétaire général de la défense et de la sécurité nationale est chargé, au nom du Premier ministre, du pilotage de la politique de sécurité des systèmes d'information de l'État. Il s'appuie, pour remplir cette mission, sur un service à compétence nationale qui lui est rattaché : l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui a le pouvoir d'ordonner aux administrations et aux opérateurs d'importance vitale de prendre les mesures de défense adaptées en cas d'attaque. Ce positionnement élevé fait la force du modèle national : placée, par son rattachement au SGDSN, auprès du Premier ministre, l'ANSSI remplit une mission interministérielle, à immédiate proximité des plus hautes autorités de l'État. Elle agit exclusivement en cyberdéfense. Elle ne mène jamais d'attaque ou d'activité de renseignement, à la différence de certaines agences étrangères qui mêlent activités offensives et défensives. En revanche, son rattachement au SGDSN place clairement l'ANSSI dans la chaîne de la défense et de la sécurité nationale, dont elle est devenue un maillon important. L'ANSSI assure, sous le pilotage du SGDSN, une fonction globale de prévention et de réaction aux attaques contre la société de l'information, avec une action orientée prioritairement vers les services de l'État et les opérateurs d'importance vitale.

Faire face à une menace en évolution permanente

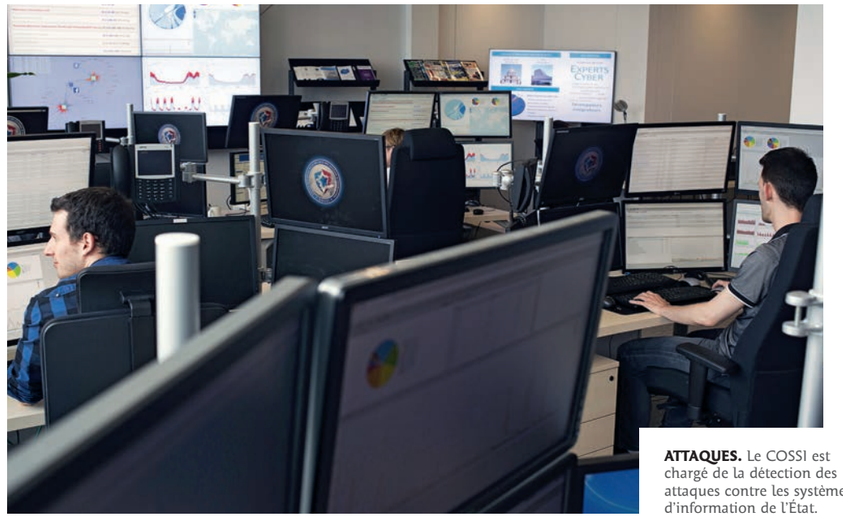
À mesure que se développe la société numérique, les attaques se multiplient contre les systèmes d'information de l'État, des opérateurs d'importance vitale, des entreprises, des collectivités territoriales, etc. La menace est multiple et prend la forme de la cybercriminalité, avec la multiplication des "rançongiciels", ces virus qui chiffrent l'information pour rançonner leurs victimes ; du vol d'informations, le plus souvent à des fins économiques ; du cybersabotage contre les opérateurs d'importance vitale (transports, télécoms, électricité...), etc. L'apparition de nouvelles menaces, comme lors de l'élection présidentielle américaine, impose à l'ANSSI de s'adapter en permanence. C'est le prix à payer pour qu'elle remplisse, dans la durée, ses deux missions essentielles : la protection, qui regroupe les mesures destinées à garantir la disponibilité, la confidentialité et l'intégrité des systèmes d'information ; la défense, qui consiste à détecter l'attaque et à réagir au plus vite pour en limiter les effets. Pour adapter la stratégie nationale en matière de sécurité des systèmes d'information, un comité stratégique, présidé par le SGDSN, réunit les principales autorités en charge de la sécurité nationale et de la société de l'information.

Typologie de menaces majeures

1. La cybercriminalité
2. Le vol d'informations économiques
3. Le cybersabotage d'activités essentielles
4. La déstabilisation politique

Les outils de communication sécurisée de l'État

OSIRIS : téléphonie fixe
ISIS : intranet et messagerie
HORUS : visioconférence
SECDROID : téléphonie mobile



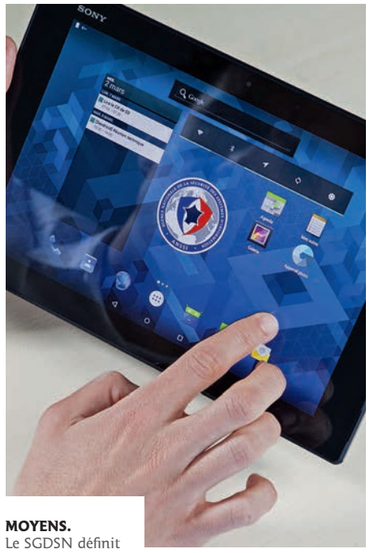
ATTAQUES. Le COSSI est chargé de la détection des attaques contre les systèmes d'information de l'État.

COSSI, les « pompiers » du cyberespace

En 2016, une vingtaine d'attaques de grande ampleur ont été enregistrées. C'est le centre opérationnel de la sécurité des systèmes d'information (COSSI) qui est chargé de détecter et de réagir au plus tôt en cas d'attaque informatique. Il est doté – depuis le 3 octobre 2016 – d'un point de contact unique, accessible 24 heures sur 24 et 7 jours sur 7. Au-delà de sa fonction de veille et d'analyse, visant à comprendre les attaques en comparant les modes opératoires, le COSSI exerce sa capacité de détection grâce aux sondes de protection des réseaux de la présidence de la République, des services du Premier ministre et des ministères. Ces sondes sont des capteurs qui permettent de repérer et d'identifier très vite les signaux d'attaque, puis de déclencher l'intervention et le traitement de l'incident. En 2016, les équipes du COSSI sont intervenues auprès d'opérateurs divers, intervenant dans plusieurs secteurs de l'économie. L'action de l'ANSSI auprès des cibles attaquées se prolonge ensuite dans la durée, jusqu'à ce que les systèmes infectés soient totalement rétablis.

En interaction permanente avec le sommet de l'État

L'ANSSI assure une information permanente des plus hautes autorités de l'État sur les attaques et les opérations de cyberdéfense en cours. Un état de la situation leur est régulièrement présenté ainsi que l'état des opérations menées par le COSSI. De plus, une analyse technique des attaques ainsi que de leurs possibles conséquences est communiquée. Les analyses sont ensuite partagées avec les victimes des attaques. En 2016, l'ANSSI a été impliquée dans la préparation de l'Eurofoot, comme elle l'avait été en décembre 2015 dans l'organisation de la COP21. Aujourd'hui, l'ANSSI est systématiquement associée à la prévention et à la gestion des crises, éventuellement *via* la cellule interministérielle de crise (CIC).



MOYENS. Le SGDSN définit les solutions de communication sécurisée dont sont dotées les plus hautes autorités de l'État.

Guillaume POUPARD, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Travaillons en réseau avec nos partenaires européens

2016

« Nous considérons qu'il est de notre responsabilité de développer la cybersécurité au niveau international. Les frontières du cyberespace étant très floues, il n'est plus possible de se cantonner à des logiques purement nationales. Notre principal enjeu, en 2016, était de convaincre nos partenaires européens de travailler en réseau. La directive européenne *Network and Information Security* (NIS), approuvée le 6 juillet 2016, va nous aider car elle prévoit que tous les États membres doivent se doter de centres nationaux comparables à notre centre opérationnel de sécurité des systèmes d'information (COSSI). Nous aurons ainsi des homologues dans tous les pays européens pour traiter ensemble les questions de cybersécurité. »

PROSPECTIVE

« Les équipes de l'ANSSI réfléchissent aux sujets de sécurité soulevés par le développement du véhicule autonome, à la mise en place d'une assurance liée au cyber-risque et à la complexité de la ville intelligente, où tous les systèmes seront connectés. L'ANSSI travaille également sur la question du droit international dans le cyberespace. Nous avons milité avec succès pour que cet espace ne soit pas considéré comme une zone de non-droit. »

DROIT DE LA PAIX

«Le SGDSN a ceci de particulier : nous collaborons avec des chercheurs et des spécialistes du droit international pour définir les règles qui devraient s'appliquer internationalement. Jusqu'ici, beaucoup de travaux ont été menés sur la transcription du droit de la guerre vers le cyberespace. Il est temps de s'intéresser aussi au droit de la paix. L'ANSSI a préparé la première conférence internationale « Construire la paix et la sécurité », qui s'est tenue en avril 2017 à Paris. Cette première édition visait à à donner un élan pour initier un premier corpus de règles. C'était aussi l'occasion d'offrir une meilleure visibilité aux positions de la France en matière de construction de la paix par le droit dans un monde en transition numérique. »

Des solutions de pointe pour une efficacité maximale

En étroite coopération avec le centre de transmissions gouvernemental (CTG), lui aussi rattaché au SGDSN, l'ANSSI participe à la modernisation et à la sécurisation des moyens de communication interministérielle. Au premier semestre 2016 a été mené un travail de définition des solutions de téléphonie fixe, à la fois ergonomiques et hautement sécurisées, qui seront mises à la disposition des hautes autorités de l'État. Puis a été lancée la construction du nouveau matériel retenu, appelé OSIRIS, qui entrera en service à l'été 2017. Par ailleurs, des travaux ont été engagés pour améliorer le réseau ISIS : cet intranet interministériel, homologué au niveau « Confidentiel défense », offre à ses 4100 utilisateurs un service de messagerie, un portail d'information et de partage de documents, un annuaire interministériel de crise et une base de données cartographiques. L'ANSSI et le CTG ont aussi poursuivi le déploiement dans différentes entités ministérielles de la solution de visioconférence sécurisée HORUS, déjà en place à la présidence de la République, à Matignon et dans certains centres de crise. HORUS présente la particularité d'être interconnecté avec les systèmes de certains pays alliés, ce qui permet des visioconférences au plus haut niveau.
Des solutions de téléphonie mobile ont aussi été élaborées par l'ANSSI. La diffusion des ordiphones sécurisés SECDROID a ainsi été élargie au sein du SGDSN, du ministère de la justice et de la préfecture de police de Paris notamment. Enfin, l'ANSSI a accompagné la direction générale de la gendarmerie nationale dans la mise à disposition de ses terminaux de communication et de travail nomades (NEOGEND), distribués à plusieurs milliers de gendarmes.

PSSIE. Les équipes de l'ANSSI ont élaboré la politique de sécurité des systèmes d'information de l'État, adoptée par l'ensemble des ministères.

Assurer la sécurité des réseaux nationaux de communication

L'article 226-3 du code pénal soumet à autorisation la commercialisation et la détention d'équipements susceptibles de porter atteinte à la confidentialité des communications électroniques. Ce régime de contrôle a été étendu en 2016 aux « stations de base », qui assurent la desserte radio des réseaux de téléphonie mobile. Cette mesure permettra d'anticiper les évolutions technologiques de ces réseaux, et notamment l'arrivée de la 5G. L'ANSSI, qui joue un rôle central dans le contrôle réglementaire, a contribué à cette évolution, comme à celle de tous les textes relatifs à la sécurité et à la défense des systèmes d'information. En 2016, elle a transmis aux opérateurs télécoms ses premières recommandations au sujet du déploiement des services VoLTE, qui permettent de passer des appels *via* la 4G, ce qui n'était jusqu'alors pas possible.

Des systèmes sécurisés pour l'administration

La sécurité des systèmes d'information de l'administration mobilise une partie importante des équipes de l'ANSSI. L'agence est en effet directement associée à chacun des grands projets numériques de l'État. En 2016, ses compétences en matière d'assistance ont été consacrées en priorité aux grands projets interministériels : refonte des systèmes d'information de l'administration territoriale de l'État (ATE), chantiers de sécurisation et d'urbanisation liés à la mise en œuvre du réseau interministériel de l'État (RIE), projets interministériels d'« informatique dans les nuages », mise en place de France Connect, l'outil d'identification sécurisé développé pour faciliter l'accès aux téléservices proposés par l'administration, etc. À eux seuls, ces projets emblématiques ont représenté près de 30 % de l'activité d'assistance de l'ANSSI aux administrations et aux opérateurs d'importance vitale. L'administration bénéficie aussi de l'installation progressive de produits de confiance, labellisés par l'ANSSI, en matière de chiffrement ou de téléphonie mobile notamment.

FRANCE connect

L'An II de la PSSIE

Elaborée par l'ANSSI, la politique de sécurité des systèmes d'information de l'État (PSSIE) a été détaillée dans une circulaire signée par le Premier ministre le 17 juillet 2014. Elle décline dix principes fondamentaux portant sur le choix d'éléments de confiance pour construire les systèmes d'information, sur la gouvernance de la sécurité et sur la sensibilisation des acteurs. Parmi ces principes, la circulaire met en avant la nécessité pour les administrations de l'État de recourir à des produits et à des services qualifiés par l'ANSSI ainsi qu'à un hébergement sur le territoire national de leurs données les plus sensibles.
2016 est la seconde année complète d'application de cette politique : la PSSIE a été adoptée par l'ensemble des ministères, sous le pilotage de leurs hauts fonctionnaires de défense et de sécurité. Dans le prolongement des décrets d'application de la loi de programmation militaire publiés en 2015, neuf arrêtés sectoriels ont été pris en 2016 par les ministères concernés.

Chiffrement pour 600 000 postes

Fin 2016, plus de 600 000 postes informatiques de l'administration ont été équipés d'outils de chiffrement de grande qualité, pour un coût quasiment nul.

450
millions d'euros

C'est l'enveloppe budgétaire de la Commission européenne consacrée au cyberpartenariat public-privé signé avec ECSO pour développer la R&D en cybersécurité.

DIRECTIVE. L'Union européenne a adopté la directive NIS, qui prévoit que tous les pays membres fassent l'effort de se mettre au même niveau en matière de cybersécurité.

Oui à la coopération ; prudence quant à la localisation des données

Face aux menaces, la démarche de sécurisation des systèmes d'information ne peut plus se limiter aux frontières de l'Hexagone. Le caractère transnational des menaces des opérateurs importants, l'interconnexion des réseaux imposent des coopérations avec les partenaires européens de la France. L'année 2016 a, sur ce sujet, marqué un tournant. Les coopérations bilatérales se sont intensifiées avec l'Allemagne et la Grande-Bretagne. L'enjeu est que tous les pays européens fassent un effort de mise à niveau en termes de cybersécurité pour permettre un véritable travail en réseau. La directive NIS, adoptée le 6 juillet 2016, va dans ce sens : elle prévoit que l'ensemble des États membres doivent se doter de centres nationaux de sécurité des systèmes d'information, ce qui n'est pas le cas à ce jour.

Le cyberpartenariat public-privé signé entre la Commission européenne en 2016 (cPPP) et l'association ECSO constitue, quant à lui, un pas important dans le sens de l'autonomie stratégique de l'Europe en matière de cybernétique. Ce partenariat vise à rassembler des représentants de l'ensemble des acteurs du domaine pour soutenir la recherche et le développement en matière de cybersécurité. Une enveloppe de 450 millions d'euros est financée par la Commission, qui en attend un fort effet de levier : au total, près de 2 milliards d'euros pourraient être mobilisés.

Au plan international, le SGDSN et l'ANSSI se sont mobilisés pour étudier l'impact des traités de libre-échange, comme le projet d'accord de libre-échange entre les États-Unis et l'Union européenne (TAFTA) sur la cybersécurité. Se pose notamment la question du *free flow of data*, qui prône la « libre circulation » de toutes les données. La France considère ce principe comme très contestable. Elle insiste sur la nécessité de conserver le contrôle du pays d'hébergement des données, notamment les plus sensibles.

Promouvoir la confiance numérique

Au-delà des sujets de souveraineté nationale, la société et les acteurs économiques ont pris conscience que le développement numérique ne peut se concevoir sans cybersécurité. Pour ce faire, l'ANSSI mène des actions de politique industrielle visant à consolider la filière nationale de sécurité informatique, en s'appuyant sur le cadre proposé par la Nouvelle France industrielle, dont le 33e plan (« Plan 33 ») porte sur l'industrialisation de la France en matière cybernétique. De nombreuses actions concrètes ont été lancées en termes de financement (via le programme des Investissements d'avenir), de labellisation (avec la création du label France Cybersecurity qui valorise les produits de confiance), de formation (par la labellisation de formations supérieures en sécurité numérique), de réglementation, etc.

Des avancées majeures dans le référencement de prestataires de confiance sont à signaler. Elles permettent de démultiplier des interventions jusqu'alors prises en charge par l'ANSSI. En 2016, l'ANSSI a aussi « incubé » le futur dispositif d'assistance aux victimes d'actes de cybermalveillance (ACYMA). Ce nouveau dispositif a vocation à devenir autonome sous la forme d'un groupement d'intérêt public (GIP), d'abord financé par l'ANSSI, puis progressivement par des acteurs privés.

PIRANET 16

Organisé en décembre 2016 par le SGDSN avec la participation active de l'ANSSI, PIRANET 16 constituait le premier exercice gouvernemental majeur de cyberattaque mettant en jeu le fonctionnement de l'État *(lire p. 12).*

CONTRÔLER et CERTIFIER

La lutte contre la prolifération des armes de destruction massive, la protection des technologies sensibles, le contrôle des exportations de matériels de guerre, la maîtrise des données spatiales sont devenus des enjeux majeurs pour la défense et la sécurité nationale. Au sein de l'administration, le SGDSN joue un rôle important dans leur prise en compte. C'est ainsi que, par délégation du Premier ministre, il délivre des licences d'exportation de matériels de guerre, contribue à des coopérations fructueuses dans le domaine de l'armement, notamment avec les partenaires allemand et britannique, et porte les positions de la France dans les enceintes internationales qui traitent de ces questions.

La CIEEMG, point de passage obligé pour l'exportation des matériels de guerre

L'exportation de matériels de guerre est soumise à l'obtention d'une licence délivrée par l'État. Le système est interministériel : l'autorisation est donnée par le Premier ministre ou, par délégation de celui-ci, par le secrétaire général de la défense et de la sécurité nationale, sur avis de la commission interministérielle pour l'étude des exportations des matériels de guerre (CIEEMG). Cette commission, qui réunit chaque mois des représentants des ministères de la défense, des affaires étrangères, de l'économie et des finances sous la présidence du SGDSN, instruit les nombreux dossiers qui lui sont soumis avant de délivrer un avis.

Un système encadré pour une politique responsable

Le dispositif permet la mise en œuvre dans de bonnes conditions d'une politique d'exportation responsable qui s'inscrit dans un effort global de maîtrise des armements. Respectueuse de ses engagements internationaux, la France prend en compte, dans les travaux de la CIEEMG, le risque militaire induit par les armes exportées et la nécessaire protection des technologies sensibles françaises.

45 jours pour une licence

La CIEEMG délivre un avis dans un délai moyen de 45 jours, grâce notamment à la dématérialisation des procédures mise en place dans le système SIGALE.

Le processus de contrôle s'attache à concilier rigueur et fluidité pour réduire les délais de traitement des dossiers et éviter les charges inutiles pesant sur les entreprises. L'exportation est en effet vitale pour maintenir le niveau des compétences industrielles, que les commandes nationales ne peuvent suffire à financer.

Le cadre des décisions proposées par la CIEEMG au Premier ministre est déterminé par des directives de haut niveau concernant certains pays et des technologies particulières : ces directives ont été actualisées début 2017, au terme d'une consultation interministérielle menée par le SGDSN et validée par le cabinet du Premier ministre. Le SGDSN a aussi piloté des travaux interministériels d'adaptation de la réglementation en matière de contrôle des armements et d'actualisation de la liste des équipements considérés comme des matériels de guerre et assimilés.

Un fort dynamisme à l'exportation

Les demandes de licences d'exportation représentent un flux très soutenu : 6 700 demandes ont été traitées en 2016. Dans les faits, environ 95 % des demandes font l'objet d'un traitement dématérialisé en procédure continue avec avis favorable. Le reliquat, qui concerne les cas les plus sensibles, est étudié en séance plénière de la CIEEMG. En 2016, 245 demandes ont été ainsi discutées en commission. Au bilan, 2 % des demandes font l'objet d'un refus et 50 % font l'objet d'un avis favorable assorti de conditions particulières permettant de mieux encadrer l'opération d'exportation. L'importance du flux est directement liée au dynamisme des exportations françaises de matériels de guerre. Ce dynamisme s'explique notamment par l'investissement des autorités françaises en soutien des industriels et l'établissement de véritables partenariats de défense avec les États clients, qui débouchent sur la signature de contrats importants, par exemple avec l'Inde pour les Rafale et l'Australie pour les sous-marins.

L'autonomie stratégique comme priorité

Dans sa démarche d'accompagnement des exportations, le SGDSN fait de l'autonomie stratégique une priorité. Sur certaines capacités, la France évite de se retrouver en situation de dépendance vis-à-vis de pays auxquels elle devrait acheter des composants ou des sous-systèmes. C'est la démarche dite de « désensibilisation ». Sur ces sujets, le SGDSN est en dialogue constant avec la direction générale de l'armement (DGA), les entreprises et les ministères pour faire converger les intérêts de la défense nationale et les logiques industrielles. La recherche d'autonomie stratégique n'exclut pas de nouer des partenariats industriels structurants avec d'autres pays. Une avancée importante a été réalisée dans ce sens avec le Royaume-Uni : en 2016, les parlements des deux pays ont ratifié l'accord intergouvernemental qui met en place le système « One MBDA ». Au terme de cet accord, Français et Britanniques produisent ensemble des systèmes de missiles et créent une véritable synergie industrielle et des économies d'échelle. Le système est sécurisé par le principe d'interdépendance, qui prévoit qu'aucun des deux pays ne peut bloquer les exportations de l'autre à destination de pays dont la liste a été réciproquement approuvée. Cette coopération industrielle s'inscrit dans la même logique que le projet KANT, étroitement suivi par le SGDSN, qui a abouti au rapprochement du français Nexter et de l'allemand Krauss-Maffei Wegmann, finalisé en décembre 2015. Le nom du nouveau groupe, KNDS, a été rendu public au cours du salon Eurosatory en juin 2016, à Villepinte.

Partenariat Le projet « One MBDA » crée une véritable synergie industrielle entre la France et le Royaume-Uni.

COOPÉRATION. Le rapprochement du Français Nexter (fabricant du VBCI, photo ci-dessous) avec l'Allemand Krauss-Maffei Wegmann donne naissance au nouveau groupe KNDS.

Contre la prolifération, sur tous les fronts

La France a fait de la lutte contre la prolifération des armes de destruction massive une des priorités de sa politique étrangère et de défense. L'effet déstabilisateur de la prolifération sur la sécurité internationale est accentué par le fait qu'elle se développe dans des zones de tension, comme le Moyen-Orient ou l'Asie. La France agit dans un cadre multilatéral et, à chaque fois que c'est nécessaire, par des initiatives *ad hoc*. Le SGDSN a un rôle d'animateur et de coordonnateur interministériel dans le dispositif national mis en place pour lutter contre la prolifération. Sa direction des affaires internationales, stratégiques et technologiques assure une veille permanente dans les domaines concernés : nucléaire, radiologique, biologique, chimique, explosifs, missiles et spatial. Elle coordonne les études sur

« One MBDA », intégration réussie

Fruit du traité de Lancaster House signé en 2010 par Paris et Londres, le projet « One MBDA » donne naissance à un acteur européen unique dans le domaine des missiles, tout en préservant l'autonomie stratégique des deux partenaires.

Anticiper les risques et assurer le suivi des menaces

Frédéric JOURNÈS,
directeur des affaires internationales, stratégiques et technologiques (AIST) au SGDSN

2016

« Cette année s'est caractérisée par un degré très élevé d'incertitude. Les premiers mois ont été dominés par les phénomènes terroristes qui ont induit pour la direction AIST un très important travail sur l'anticipation des risques et le suivi des menaces contre notre territoire. La fin de l'année a, elle, été dominée par le retour à un rapport de puissance dans les relations avec des pays comme la Chine ou la Russie. Elle a aussi été marquée par un questionnement sur la relation avec certains de nos alliés, suite à l'annonce de la sortie des Britanniques de l'Union européenne et aux positions prises par le nouvel exécutif américain. »

PRIORITÉS

« Nous avons été fortement sollicités pour réaliser un travail de synthèse sur les questions terroristes afin d'alimenter les conseils de défense, qui sont devenus hebdomadaires après l'attentat de Nice. Nous nous sommes également concentrés sur le projet « Galileo », qui constitue un enjeu majeur pour assurer l'autonomie européenne en termes de navigation satellitaire. Plus globalement, toutes nos actions sont motivées par la nécessité de contribuer à la stabilité et la sérénité de la prise de décision publique, dans une période qui n'incline pas à la confiance. Le SGDSN se distingue par sa capacité à réfléchir à moyen terme. C'est pourquoi, dans nos missions de coordination interministérielles, nous veillons à apporter de la pondération en plus de la compétence technique. »

RESSOURCES

« La direction AIST peut compter sur des collaborateurs aguerris et très investis
Sur des sujets que j'appellerais "le cœur du réacteur", le ministère de la défense nous envoie des militaires de très haut niveau. Ils peuvent s'appuyer sur une équipe performante, étoffée par des contractuels de grand talent, des jeunes issus de Sciences Po ou du monde universitaire par exemple. »

NUCLÉAIRE. Les exportations de technologies sensibles font l'objet d'une supervision spécifique par le SGDSN.

la prolifération des armes de destruction massive et produit des documents de synthèse sur les sujets d'actualité comme l'Iran ou la Syrie.
Par ailleurs, le SGDSN assure le secrétariat du Comité interministériel pour l'application de la convention sur l'interdiction des armes chimiques (CIAC). Dans le domaine biologique, il coordonne les travaux interministériels portant sur les enjeux de sécurité et de défense liés à la biologie de synthèse – un domaine en pleine expansion– ainsi que la coopération avec les États-Unis sur la défense biologique.
Le SGDSN assure aussi la coordination de la réponse nationale aux interceptions réalisées dans le cadre de la PSI *(Proliferation Security Initiative)*. Cette coopération internationale vise à intercepter, sous le pilotage opérationnel des services du SGDSN, les cargaisons proliférantes partout dans le monde et quels que soient leurs modes de transport. Depuis l'été 2016, le SGDSN assure également la coordination des interceptions d'armements conventionnels, dans un cadre strictement national cette fois.

Article 90, pour accompagner l'export

Une procédure de réduction des risques à l'exportation existe : la procédure dite « de l'article 90 », qui tire son nom de la loi du 21 décembre 1967. Elle vise à favoriser l'exportation en réduisant le risque assumé par les industriels dans la phase d'industrialisation. Sous forme de financement public, partiel et remboursable au fur et à mesure des ventes, ce dispositif a été orienté dans une double direction ces dernières années : le soutien aux petites et moyennes entreprises et aux entreprises de taille intermédiaire ; le soutien aux grands groupes intervenant sur des projets stratégiques. La commission de l'article 90 se réunit en moyenne tous les deux mois sous la présidence du SGDSN. Au 31 décembre 2016, les encours représentaient 94,4 millions d'euros, mobilisés au bénéfice de 70 programmes en cours d'exécution par 33 entreprises.

Technologies sensibles : exportation sous surveillance

Au-delà du contrôle des exportations de matériels de guerre, le SGDSN assure aussi, pour le compte du Gouvernement, la supervision industrielle de certains domaines technologiques particulièrement sensibles. C'est le cas notamment dans le domaine du nucléaire civil : par exemple, en 2016, le SGDSN a accompagné les opérations commerciales avec la Chine. Ses équipes spécialisées se sont chargées du travail d'instruction du processus intergouvernemental franco-chinois et ont participé à une série d'exercices avec le Commissariat à l'énergie atomique et aux énergies alternatives (CEA), l'Agence des participations de l'État (APE), le ministère des affaires étrangères, etc. Objectif : cadrer au plus serré, par des accords intergouvernementaux, les possibilités ouvertes aux entreprises en matière de vente de matériel nucléaire.

Transferts intracommunautaires

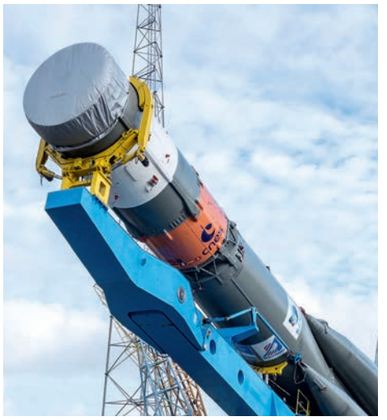
Au niveau national, le SGDSN a coordonné les travaux visant à alimenter la directive européenne du 6 mai 2009 sur les transferts intracommunautaires de produits liés à la défense – dite « directive TIC » –, par un renforcement de la mise en œuvre des licences générales de transfert à destination des forces armées et des entreprises certifiées, et par l'élaboration d'une définition des matériels spécialement conçus pour un usage militaire, qui faciliterait les procédures de classement des matériels de guerre pour les industriels.
Au-delà, le SGDSN participe activement aux échanges entre pays européens et anime le sous-comité de l'accord-cadre « *Letter of Intent* ». Ce partenariat, signé en 1998 par les ministres de la défense des six principaux producteurs d'armement en Europe (Allemagne, Espagne, France, Italie, Royaume-Uni et Suède), vise à faciliter les transferts d'armement entre les pays signataires.

Le nécessaire contrôle des biens à double usage

Au-delà des matériels de guerre clairement identifiés comme tels, se pose la question des biens à double usage, aussi appelés « BDU » : des équipements et des technologies susceptibles d'être utilisés à des fins militaires ou pouvant participer au développement, à la production, au fonctionnement d'armes de destruction massive. Ces biens sensibles peuvent faire peser une menace sur les populations. Il est donc nécessaire de contrôler leur commerce, quand bien même ils sont officiellement acquis pour des utilisations strictement civiles. À l'échelle européenne comme au plan international, la France s'implique activement dans le renforcement des régimes de contrôle à l'exportation des biens à double usage. Le SGDSN y apporte sa contribution en s'associant à la définition de la position française en vue des négociations internationales sur ces sujets – Arrangement de Wassenaar, Groupe Australie, *Missile Technology Control Regime* et *Nuclear Suppliers Group* – et en instruisant, pour le compte de la commission interministérielle des biens à double usage (CIBDU), les dossiers sensibles.

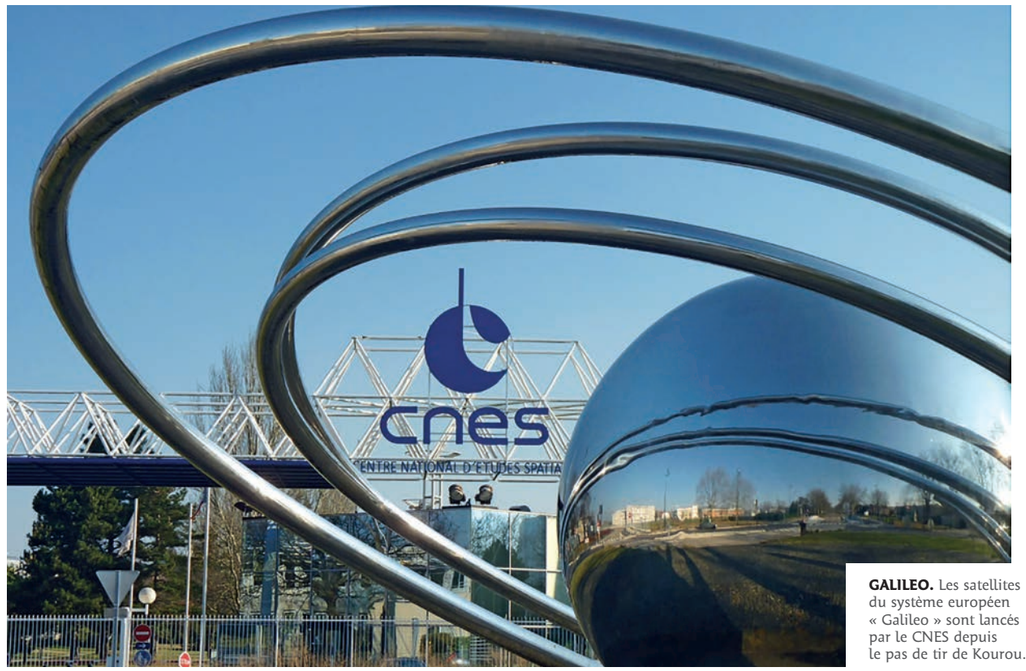
« Galileo » : garantir l'autonomie de l'Europe pour ses communications

Le 15 décembre 2016 était mis en service le système de navigation par satellites européens « Galileo », le service de géopositionnement le plus précis au monde, alternative au GPS américain. Avec « Galileo », l'Europe a fait le choix de se doter d'un système propre de satellites pour garantir la sécurité de ses communications civiles et militaires. Ce système constitue un enjeu important en termes d'autonomie pour les pays de l'Union européenne, au premier rang desquels la France, moteur du projet depuis son lancement en 1999. C'est le SGDSN qui est chargé de la coordination interministérielle sur ce projet et qui assure la cohérence des positions nationales sur les questions liées à la sécurité du système. Les signaux émis par le système « Galileo » sont notamment utilisés pour offrir un service public réglementé (PRS) réservé aux utilisateurs autorisés par les gouvernements, pour les applications sensibles ; le SGDSN assume la fonction d'autorité responsable du PRS pour la France.



« Galileo », un « GPS européen »

Mis en service en décembre 2016, le système « Galileo » permet un géopositionnement au mètre près, 10 fois plus précis que celui proposé par le GPS américain.



GALILEO. Les satellites du système européen « Galileo » sont lancés par le CNES depuis le pas de tir de Kourou.

Coordonner et Piloter | Protéger et Sécuriser | Contrôler et Certifier | Éclairer et Planifier

ÉCLAIRER et PLANIFIER

La capacité de l'État à répondre efficacement à une menace protéiforme et en évolution permanente dépend de son aptitude à identifier les risques en amont et à planifier les réponses opérationnelles adéquates. Le SGDSN s'emploie à éclairer la décision des plus hautes autorités de l'État en animant les travaux interministériels d'anticipation des menaces, d'actualisation des plans gouvernementaux, de sûreté des installations sensibles et de protection du secret de la défense nationale.

Plan VIGIPIRATE : une nouvelle version avec 3 niveaux d'alerte

Pour faire face à une menace en perpétuelle mutation, l'État doit examiner en permanence la pertinence de ses plans et l'efficacité de sa réponse. Le SGDSN y a contribué en 2016 en publiant une nouvelle version de VIGIPIRATE. Fort de 300 mesures qui peuvent être déclenchées en cas de besoin, ce plan est au cœur du dispositif de protection face à la menace terroriste ; c'est le seul plan national dont la mise en œuvre est permanente. Il propose à l'ensemble des acteurs étatiques des mesures opérationnelles et constitue un outil complet qui peut être ajusté avec précision au gré des circonstances.

La nouvelle version de VIGIPIRATE, publiée en décembre 2016, intègre les leçons tirées de l'expérience des attentats et les évolutions législatives adoptées par le Parlement, qui ont fait entrer dans le droit positif des mesures jusqu'alors liées à l'état d'urgence. Elle réarticule le plan en trois niveaux d'intervention : le niveau 1 (« Vigilance ») correspond à la posture permanente de sécurité ; le niveau 2 (« Sécurité renforcée-Risque attentat ») répond aux besoins d'une protection renforcée liée à une menace élevée ; le niveau 3 (« Urgence attentat ») déclenche un état maximal de vigilance et de protection en cas d'attaque imminente ou suite à un attentat.

Cinq postures VIGIPIRATE diffusées en 2016

Le Premier ministre fixe la posture VIGIPIRATE, qui adapte aussi souvent que nécessaire le dispositif de vigilance, de prévention et de protection, en fonction de l'état de la menace. Cette posture est déclinée en priorités et en mesures à prendre dans un document confidentiel adressé par le SGDSN à chaque ministère. Au cours de l'année 2016, cinq postures ont été arrêtées par le Premier ministre et diffusées par le SGDSN : la première en janvier, la deuxième en mars après les attentats de Bruxelles, la troisième en juin afin de prendre en compte l'organisation de l'Eurofoot, la quatrième en juillet après l'attentat de Nice, la cinquième en septembre à l'occasion de la rentrée scolaire.

VIGIPIRATE. Le SGDSN a publié en 2016 une nouvelle version du plan pour intégrer les leçons tirées des attentats.

Diffuser la culture de la sécurité auprès de la population

Le nouveau plan VIGIPIRATE s'accompagne de l'ambition de diffuser auprès de la population une culture de la vigilance. Objectif : faire comprendre que la sécurité n'est pas le monopole des forces de l'ordre, mais l'affaire de tous. Un message porté par la campagne de sensibilisation « Comment réagir en cas d'attaque terroriste ? », lancée en mars par le Gouvernement et déclinée au travers d'une série de documents ciblés. Le SGDSN a conçu et réalisé, avec le service d'information du Gouvernement (SIG) et les ministères, 11 guides de bonnes pratiques, largement diffusés vers les mairies, les établissements scolaires, les centres commerciaux, les musées, les salles de spectacle, etc.

Le lancement, le 7 juin 2016, par le ministère de l'intérieur et le SIG d'une application pour téléphone, SAIP, participe lui aussi de cette démarche d'alerte et d'information de la population.

Alerte sur téléphone

Disponible sur Apple Store et Google Play, l'application gratuite SAIP permet à chacun d'être alerté sur son téléphone mobile en cas de suspicion d'attentat.

SAIP

LE NOUVEAU PLAN VIGIPIRATE EN CHIFFRES

3 niveaux d'intervention

300 mesures

13 domaines d'action (transports, santé, réseaux…)

OPÉRATION SENTINELLE. Les conditions d'emploi des militaires de la force Sentinelle ont été redéfinies en 2016 par le SGDSN.

La famille des plans PIRATE remise à jour

Au-delà de VIGIPIRATE, un catalogue de plans complémentaires, regroupés dans la famille « PIRATE », a été élaboré pour répondre à la menace terroriste. Ces plans d'intervention ont vocation à être activés en cas d'attaque dans un cadre particulier comme le milieu aérien, maritime ou le cyberespace. Le SGDSN travaille à l'amélioration permanente de ces outils de planification en élaborant des plans de nouvelle génération conçus comme des aides à la décision, facilitant la compréhension de situations complexes. Trois d'entre eux ont fait l'objet d'une mise à jour en 2016 : NRBC, PIRANET et PIRATE-MER. Dans l'optique de la compétition Eurofoot, le SGDSN a diffusé une version provisoire des plans PIRANET (cybersécurité) et NRBC (risque nucléaire, radiologique, chimique et bactériologique), dans l'hypothèse où des menaces de cette nature se concrétiseraient. La rénovation du plan NRBC a été menée à bien fin 2016. Fondée sur une nouvelle évaluation des menaces maritimes, diffusée en juillet, la révision du plan PIRATE-MER a, elle aussi, été menée à bien. Enfin, la nouvelle version du plan PIRANET, qui permet d'intervenir en cas d'attaque contre les systèmes d'information, prend en compte les expériences tirées de l'exercice majeur « PIRANET 16 » *(lire p. 12)* organisé en décembre 2016.

10 000

militaires mobilisés pour Sentinelle

Le dispositif Sentinelle organise le déploiement des forces armées sur le territoire pour protéger la population. Il a été dynamisé et précisé au cours de l'année 2016.

Optimiser l'emploi de la force Sentinelle

Depuis les attentats de janvier 2015, entre 7000 et 10 000 militaires sont engagés en permanence sur le territoire national pour protéger les Français. L'opération Sentinelle organise ce déploiement. Dans le prolongement des décisions prises le 29 avril 2015 par le Président de la République, le Premier ministre a chargé le SGDSN de réfléchir aux possibles adaptations du dispositif pour garantir la disponibilité, la capacité d'action et l'efficacité des forces engagées. Fondés sur l'expérience des mois écoulés, ces travaux ont permis de définir des évolutions à court et moyen termes. Ils sont venus enrichir le rapport relatif à l'engagement des armées sur le territoire national, remis au Premier ministre par le SGDSN. La plupart des 24 propositions avancées par le SGDSN sont entrées en application. Ces mesures ont permis de modifier l'emploi des unités militaires : utilisation dynamique ; moindre recours aux gardes statiques ; fin de la territorialisation des interventions du RAID et du GIGN ; évolution des conditions d'ouverture du feu, etc.

Sécuriser les activités d'importance vitale

Justice, santé, transports, énergie… douze secteurs d'activité d'importance vitale (SAIV) sont définis comme indispensables à la résilience de la Nation. Afin d'organiser leur protection, 21 directives nationales de sécurité ont été approuvées par le Premier ministre. Ces directives décrivent les menaces à prendre en compte par chaque secteur d'activité, identifient les vulnérabilités, fixent les exigences de protection et déterminent les mesures à mettre en œuvre en fonction de l'intensité de la menace, en cohérence avec le plan VIGIPIRATE. Leur révision est un chantier permanent pour le SGDSN, qui œuvre à renforcer la politique de sécurité des activités d'importance vitale. Avec deux objectifs principaux : élargir la conception des directives à une approche « tous risques » et renforcer la sécurité des systèmes d'information des opérateurs, en étroite collaboration avec l'ANSSI.

L'enjeu particulier des sites « Seveso »

Le dispositif des SAIV a été complété par l'intégration en son sein de 78 sites classés « Seveso ». C'est l'une des mesures recommandées par le SGDSN dans le rapport sur la protection des sites industriels sensibles, rendu le 3 mai 2016. Le Premier ministre lui avait donné mandat pour conduire des travaux interministériels à la suite des événements survenus l'année précédente à Saint-Quentin-Fallavier puis à Berre-l'Étang. Les recommandations de la mission d'inspection sur la publication d'informations sensibles relatives aux installations « Seveso » ont été intégrées à la réflexion et des travaux ont été engagés dans le cadre du Comité de la filière industrielle de sécurité (CoFIS) pour faciliter l'émergence de solutions technologiques adaptées.

Drones : un usage mieux encadré et contrôlé

Le 24 octobre 2016, le Président de la République a promulgué la loi relative au renforcement de la sécurité de l'usage des drones civils. Aboutissement d'un travail mené depuis deux ans par le SGDSN, ce texte précise le cadre juridique d'une activité jusqu'alors très peu réglementée,

Nous anticipons la menace en permanence, au fil de l'année

Pascal BOLOT, directeur de la protection et de la sécurité de l'État (PSE) au SGDSN

2016

« Évidemment, cette année a été rythmée par les actes terroristes et la gestion de leurs suites, notamment au moment de l'attentat de Nice. Nous avons armé la cellule interministérielle de crise 36 jours. Dans une année normale, elle est activée 6 à 10 jours, pour des exercices ! Nous avons fait face à d'autres événements, comme la crue de la Seine, avec des risques de dysfonctionnements des ministères situés à proximité. Mais la continuité de l'appareil d'État a été maintenue. Ensuite, nous avons enchaîné avec l'Eurofoot, dont le match d'ouverture avait lieu le 10 juin. Avec une nouveauté à gérer dans un contexte très difficile : les fan zones. Le monde entier avait les yeux braqués sur nous. »

ANTICIPER

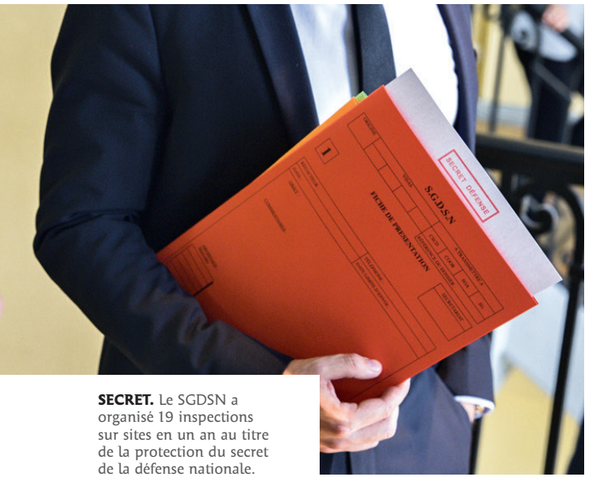
« Même si la partie la plus visible de l'action est la gestion de la crise en direct, il faut comprendre que nous anticipons la menace en permanence, au fil de l'année, et que nous planifions les réponses possibles à y apporter. Nous tirons les leçons de chaque événement ; nous organisons des exercices simulant une crise portant sur un thème sélectionné ; nous remettons à jour les plans, etc. C'est vrai pour le plan VIGIPIRATE, qui a été complètement revu, mais aussi pour les plans de réponse à la menace NRBC, de cybersécurité, de sécurité des espaces maritimes, etc. Face à une crise, nous sommes en appui de la cellule interministérielle de crise. Nous lui présentons des options et des mesures concrètes à prendre. »

ATOUTS

« Le SGDSN a ceci de particulier qu'il combine un rôle de coordination interministérielle et de fortes expertises en propre. C'est notre cas à la direction PSE : nous rassemblons des militaires de très haut niveau, des policiers et des gendarmes, des experts dans des domaines très particuliers, comme le risque bactériologique, la sécurité aérienne ou la protection du secret de la défense nationale, des médecins, des biologistes, etc. Ce creuset fait notre force. »

SURVEILLANCE. Sécuriser les activités d'importance vitale, les sites industriels sensibles, les événements d'importance… autant de missions qui mobilisent en permanence les forces de l'ordre dans le cadre de l'État d'urgence en vigueur depuis 2015.

DRONE. Encadrer l'usage des drones civils devenait une question de sécurité nationale : le SDGSN a animé les travaux préparatoires à la loi du 24 octobre 2016.



SECRET. Le SGDSN a organisé 19 inspections sur sites en un an au titre de la protection du secret de la défense nationale.

mais qui s'est développée dans des proportions importantes ces dernières années, provoquant des incidents : en 2014 et 2015, le survol de centrales nucléaires par des drones non identifiés avait inquiété et, en février 2016, un Airbus A320 d'Air France avait évité de justesse une collision avec un drone alors qu'il était en approche de Roissy. Il devenait nécessaire de remédier à cette situation.

Le SGDSN a animé un groupe de travail, conjointement avec le ministère de l'intérieur et la direction générale de l'aviation civile, pour adapter les textes et y insérer de nouvelles obligations en matière de formation, d'immatriculation, d'identification des drones, sans freiner le développement économique d'un secteur dynamique. Ses orientations ont nourri le rapport *L'essor des drones aériens civils en France : enjeux et réponses possibles de l'État*, remis le 20 octobre 2015 par le Gouvernement au Parlement, préalablement au vote de la loi n° 2016-1428 du 24 octobre 2016 relative au renforcement de la sécurité de l'usage des drones civils

Dans le même temps, il devenait indispensable de disposer de moyens efficaces de lutte contre les menaces liées aux drones. Le SGDSN a financé et conduit, en partenariat avec l'Agence nationale de la recherche (ANR), le développement de projets de contre-mesures. Les trois premiers démonstrateurs de systèmes anti-drones ont été présentés le 18 novembre 2016 sur la base aérienne de Villacoublay.

Le risque sur la biosécurité

Le secrétaire général assure la présidence du Comité national consultatif sur la biosécurité (CNCB), qu'il a contribué à mettre en place le 26 novembre 2015. Cette instance de concertation entre les milieux scientifiques et l'État est le lieu d'une réflexion partagée sur les détournements d'usage possibles des sciences du vivant et sur les moyens de s'en prémunir. En 2016, le CNCB a ainsi élaboré un rapport sur les risques associés à un usage dual de la technique de synthèse et de modification programmée des génomes.

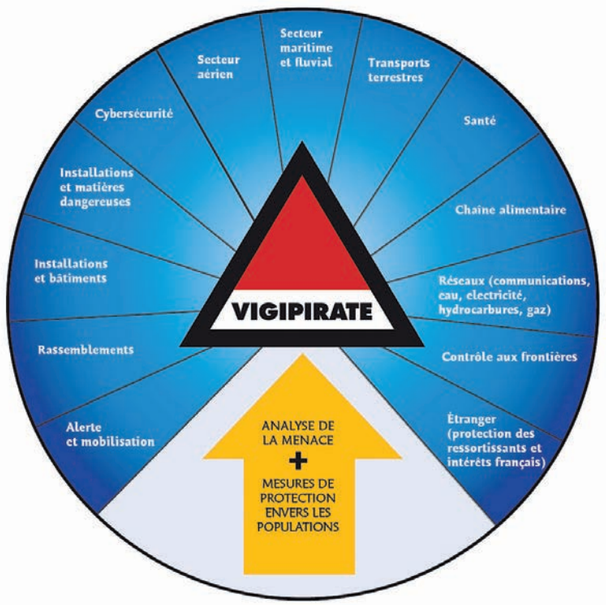
Autorité nationale de protection du secret de la défense nationale

Le SGDSN est chargé de garantir la protection du secret de la défense nationale. Cette obligation s'attache aux documents, aux personnes, aux locaux et aux réseaux, et impose le respect de règles précises auxquelles doivent se plier l'État, les entreprises et les individus. Pour s'assurer du respect de la législation en vigueur pour les informations les plus sensibles, le SGDSN organise des inspections (19 en 2016) sur des sites de l'État et au sein d'entreprises détentrices.

Des informations classifiées font l'objet d'échanges avec des entités étrangères : États, institutions internationales, entreprises, etc. Le SGDSN mène les travaux de définition des normes communes de préservation du secret de la défense avec ces partenaires. Il négocie aussi des accords généraux de sécurité avec certains pays. Un accord de ce type a été conclu récemment avec l'Australie, partenaire avec lequel la France construira 12 sous-marins d'attaque, au terme du contrat signé le 20 décembre 2016.

Au-delà, une révision de l'instruction générale interministérielle du 30 novembre 2011 (IGI 1300) est engagée. Cette instruction du Premier ministre, rédigée par le SGDSN, organise la protection du secret de la défense nationale. Des consultations interministérielles sont conduites. Les objectifs sont de mieux prendre en compte la dématérialisation des données et de rapprocher le système français de classification de celui de nos partenaires de l'OTAN.

Les 13 domaines d'action du plan VIGIPIRATE



RESSOURCES

Finances et budget, gestion des ressources humaines, logistique, infrastructures, achat public, sécurité des agents et des locaux, etc. Toutes ces fonctions de soutien sont essentielles au SGDSN et aux services qui lui sont rattachés pour assurer leur bon fonctionnement et leur permettre d'accomplir leurs missions dans les meilleures conditions.

Nous recrutons et fidélisons des talents

Philippe DECOUAIS, chef du service de l'administration générale au SGDSN

RESSOURCES HUMAINES

« La croissance de l'ANSSI et l'adossement du GIC se sont traduits par une hausse des effectifs du SGDSN de plus de 150 agents en 2016. Au regard de cet enjeu, les objectifs de réalisation du schéma d'emploi prévisionnel des effectifs et de pilotage ont pu être atteints grâce à des processus de concertation entre les acteurs. En parallèle, la politique sociale a été étendue par des mesures en matière de logement ou de garantie complémentaire santé au profit du personnel, quel que soit son statut. L'accompagnement visant à maintenir ou développer les parcours professionnels a été formalisé, notamment par des bilans de compétences, et soutenu, dans le cadre de la préparation aux concours. Un plan d'action destiné à maîtriser les risques psychosociaux, réalisé en concertation avec les représentants du personnel, a également été approuvé par le secrétaire général. Les premières mesures de formation et de communication, ainsi que le lancement d'un marché permettant la consultation de psychologues à partir d'un numéro d'appel gratuit, ont ainsi été mis en œuvre. »

BUDGET

« Les règles de gestion introduites en 2015 ont pleinement produit leur effet en 2016. L'année a été marquée par une association plus étroite des directions à la programmation et à l'exécution des crédits et des emplois, par la mise en œuvre d'une nomenclature d'activité rénovée et par la définition de centres de coûts. La dématérialisation des factures a continué de progresser, l'objectif de 20 % ayant été atteint dès le premier semestre. L'adossement budgétaire et financier du GIC a été conduit en cours de gestion, notamment pour la préparation du budget 2017. »

SOUTIEN

« La montée en puissance de missions techniques portées par l'ANSSI, le CTG ou le GIC implique une mise aux normes des installations. Ces évolutions techniques ont nécessité une programmation exigeante, des études et des opérations d'envergure : sécurisation électrique, sécurisation de l'emprise SGDSN, création de salles de serveurs informatiques, climatisation. La hausse des effectifs a aussi entraîné une adaptation des infrastructures et un redéploiement des agents. »

CHIFFRES CLÉS

RÉPARTITION DES AGENTS DU SGDSN

PAR CATÉGORIE

- A+ **361**
- A **260**
- B **193**
- C **231**

PAR STATUT

Fonctionnaires	Militaires	Contractuels
163	346	536

PAR STRUCTURES

400 agents
ont bénéficié de 1649 jours de **formation** en 2016, ce qui représente un effort budgétaire de 375 894 euros.

36400 visiteurs
sont accueillis chaque année sur les sites du SGDSN. Un détachement de sécurité de 37 gendarmes contrôle cet accès dans les conditions spécifiques liées à l'accès à des zones protégées.

150 marchés publics
étaient en cours d'exécution au SGDSN en 2016, dont 53 marchés ministériels ou interministériels dans le cadre de la politique de mutualisation des achats de l'État. En un an, le bureau achats-marchés a notifié 49 marchés ou contrats, 3 conventions avec l'UGAP, et passé 1400 bons de commande.

RPS

Le SGDSN développe un plan d'action contre les risques psychosociaux : 5 sessions de formation ont été organisées en 2016, un livret d'information a été adressé à tous les agents ainsi qu'un guide spécifique pour les managers. Une ligne téléphonique d'assistance psychologique, disponible 7 jours/7 et 24 heures/24 sera prochainement ouverte.

276,2 M€
C'est le budget 2017 du SGDSN. Sur ces 276,2 millions, 85 sont consacrés à la masse salariale.

20000 m²
de bâtiments sont occupés par le SGDSN et ses services sur quatre emprises, la principale étant située 51, boulevard de La Tour-Maubourg, au cœur du site historique de l'hôtel national des Invalides.

24 h/24 et 7 j/7

➔ Le bureau « Veille et Alerte » du SGDSN informe les autorités des événements graves.

➔ Le CTG veille au bon fonctionnement des réseaux protégés.

➔ Le point de contact du centre opérationnel COSSI, de l'ANSSI, permet de réagir au plus tôt en cas d'attaque informatique.

Secrétariat général
de la défense et de
la sécurité nationale

51, boulevard de la Tour-Maubourg - 75700 Paris 07 SP
Tél. : 01 71 75 80 00

www.sgdsn.gouv.fr