PRÉVENTION DU TERRORISME

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)
Directrice de la publication : *Claire Landais*
Coordination : *Gwénaël Jézéquel*
Conception et réalisation : *Prop'OSE et Chien Jaune studio*
prop-ose.fr - chienjaunestudio.com
Coordination éditoriale : *Stéphane Malagnac*
Crédits photos : *S.de la Moissonnière / AFP : S. De Sakutin,*
C. Petit Tesson, A. Jocard, J. Demarthon / ECPD : A. Roiné /
P. Vermes / Fotolia : vchalup, IRStone, O. Tuffé, Ö. Güvenç,
R. Wilson, neko92vl / Pléiades : CNES / Nexter / P. Gaillardin /
DICOD : F. Pellier, A. Roiné, B. Biasutto, C. Fiard /
Illustrations : *Chien Jaune studio*

SOMMAIRE

04
ÉDITO
- Louis Gautier

06
FRISE CHRONOLOGIQUE

10
REVUE STRATÉGIQUE DE CYBERDÉFENSE

11
COORDONNER & PILOTER
- 2017 : une année de transition

19
PROTÉGER & SÉCURISER
- 2017 : une année de prise de conscience

27
CONTRÔLER & CERTIFIER
- Contribuer à la sécurité internationale

35
ÉCLAIRER & PLANIFIER
- 2017 : un risque terroriste élevé et persistant

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

SGDSN

Inauguré en 2016, le rapport d'activité annuel du secrétariat général de la défense et de la sécurité nationale répond à un double objectif d'information et de transparence. Organisme aux origines anciennes, secrétariat du conseil de défense et de sécurité nationale, service du Premier ministre en charge des dossiers interministériels du champ de la défense et de la sécurité nationale, le SGDSN est à la fois un rouage important de l'État et une structure méconnue, tant en raison de la multiplicité de ses missions que du caractère confidentiel de nombre d'entre elles. C'est pour répondre au double souci d'expliquer et de faire la part des choses entre le secret et l'information publique que ce rapport a été conçu. C'est dans cette optique qu'il a été imaginé par mon prédécesseur, Louis Gautier. Cette initiative heureuse est l'une des nombreuses innovations qu'il aura portées durant ses quatre années passées à la tête du SGDSN.

Ce rapport est le sien. Il poursuit une série qui, partant de 2015, a rendu compte d'une activité très marquée par les effets de la menace terroriste sur notre pays, ses voisins européens et ses amis africains ou orientaux. Pour simplifier, je retiens que 2015 aura été l'année des plus grands drames et de la première réponse de l'État, de la dure concrétisation de menaces jusqu'alors latentes et de l'épreuve de la résilience collective du pays. L'année 2016 aura été celle du perfectionnement et du confortement des outils de prévention et de répression de la menace terroriste. L'année 2017 aura été celle de la transition institutionnelle, mais aussi de la convergence entre menace terroriste toujours présente, tentatives de déstabilisation politique par la manipulation des réseaux sociaux et aggravation brutale de la menace cybernétique, concrétisée par les vagues d'attaques informatiques Wannacry et NotPetya en juin et juillet.

Pour ma part, je retiendrai de l'année 2017 le rôle que le SGDSN a joué dans la période des échéances civiques, puis dans la transmission de dossiers importants et complexes au plus haut niveau de l'État.

C'est cette alliance de compétence, de discrétion et de gestion de la complexité qui est la marque du SGDSN.

Dans les responsabilités qui m'ont été confiées, je m'emploierai à poursuivre le travail entrepris.

Je vous souhaite une bonne lecture.

Claire Landais,
Secrétaire générale de la défense et de la sécurité nationale (SGDSN)

Louis Gautier, secrétaire général de la défense et de la sécurité nationale, octobre 2014-mars 2018

Louis Gautier, secrétaire général de la défense et de la sécurité nationale, octobre 2014-mars 2018

LOUIS GAUTIER

UNE RÉFLEXION STRATÉGIQUE AFIN DE REPENSER UN « PROJET SGDSN »

Comment qualifieriez-vous l'année 2017 ?

2017 a été une année de transition. Du processus d'organisation de l'élection présidentielle – entamé dès la fin de l'année 2016, en réalité – au scrutin législatif puis, enfin, au renouvellement des sénateurs dans la moitié des départements, les échéances civiques ont rythmé l'année. Il en a résulté un renouvellement des autorités que nous servons. Le SGDSN, au contact de ces plus hautes autorités de l'État, a porté une attention toute particulière à cette – je devrais dire ces – transition afin d'éviter tout contretemps dans l'action politique. Dans notre domaine comme dans l'art militaire, le contretemps est le début de la désorganisation d'un dispositif.

Cette année a également été marquée par le spectre de menaces pesant sur la démocratie…

Dès l'automne 2016, le SGDSN a attiré l'attention de nos autorités sur les risques pouvant peser sur les processus électoraux. Il a fallu œuvrer à la sensibilisation des équipes des candidats, notamment aux risques cybernétiques. Le secrétariat général a, à ce titre, été sollicité par le président de la Commission nationale de contrôle de l'élection présidentielle et le président du Conseil constitutionnel, juge de l'élection, afin de leur offrir un appui dans le domaine de la cybersécurité et une expertise d'ensemble face à une menace émergente.

En cela, l'ANSSI a apporté une réponse adaptée conduisant à sanctuariser le processus électoral. L'agence a su être fidèle à ce qui fait notre patrimoine génétique commun : l'alliance de la compétence technique et de la faculté d'anticipation, dans un mouvement permanent d'adaptation aux besoins nouveaux de l'État.

Peut-on considérer que le périmètre d'action du SGDSN s'est élargi ?

Je dirais plutôt que c'est le périmètre du Conseil de défense et de sécurité national qui a grandi. La réunion du Conseil, tenue hebdomadairement depuis le mois de juillet 2016, nous le confirme chaque semaine. Le secrétariat du conseil est la première des missions du SGDSN. Ceux qui préparent le dossier transmis au Président de la République, au Premier ministre et aux participants absorbent une charge de travail qui s'est encore intensifiée depuis le mois de juin. Le Conseil aura été l'un des éléments importants de cette transmission que j'évoquais précédemment.

Vous évoquez 2017 comme une année de transition et de consolidation. Quelles sont les perspectives pour 2018 ?

2018 devrait être une année de transformation pour le SGDSN dans son ensemble. Nous vivons sous la pression des évènements depuis trois ans. Nos priorités ont été opérationnelles. Aujourd'hui, je souhaite que notre maison gagne en agilité pour toujours mieux répondre aux attentes de nos autorités. J'ai lancé en 2017 une réflexion stratégique afin de repenser un « projet SGDSN ». Elle se poursuivra et devra se concrétiser en 2018. La transformation numérique du SGDSN, la prise en compte du besoin d'un centre de veille et d'alerte gouvernemental, l'achèvement de la réforme en cours sur le secret sont autant de dossiers à porter dans les prochains mois. Au-delà des questions d'organisation, je m'interroge sur l'aide que le SGDSN pourrait apporter dans la coordination d'une politique économique de sécurité et de défense nationale.

2017

UNE ANNÉE DE TRANSITION ET DE CONSOLIDATION

L'ANNÉE 2017 AURA ÉTÉ DOMINÉE PAR UNE SÉQUENCE ÉLECTORALE IMPORTANTE DURANT LAQUELLE LE SGDSN A ASSURÉ LA CONTINUITÉ DES SERVICES DE L'ÉTAT. ELLE AURA ÉGALEMENT ÉTÉ MARQUÉE PAR DE NOMBREUX CHANTIERS ET EXERCICES ILLUSTRANT L'ACTION DU SGDSN AU TRAVERS DE SES DIRECTIONS.

2017

03 — 01 Attaque contre une patrouille SENTINELLE dans le Carrousel du Louvre

07 — 02 SGDSN — Réunion SGDSN-Commission nationale de contrôle de la campagne électorale, autour de la mise en sécurité cybernétique du processus électoral

15 — 02 SGDSN — Remise au Premier Ministre du rapport d'étape sur la sécurité dans les transports

18 — 03 Attaque d'une patrouille de l'armée de l'air, aéroport d'Orly

20 — 04 Attaque terroriste sur les Champs-Elysées : un gardien de la paix tué, trois blessés

21 — 04 Publication du rapport Chocs Futurs, étude prospective à l'horizon 2030

25 — 04 Hommage national à la Préfecture de Police de Paris suite au décès du gardien de la paix Xavier Jugelé

07 — 05 Élection du Président de la République

07 - 08 — 04 Organisation du colloque « La paix dans le cyberespace », UNESCO, Paris

11 - 18 — 06 Elections législatives

19 — 06

21 — 06 Diffusion de la posture Vigipirate « Eté 2017 »

12 — 05 Cyberattaque WannaCry

27 — 06 Cyberattaque NotPetya

04 — 07 SGDSN — Organisation d'une commission interministé-rielle de sûreté aérienne (CISA) sur la politique nationale de sûreté et de défense aérienne

11 — 07 SGDSN — Remise au Premier Ministre du rapport final sur la lutte contre les menaces asymétriques

13 — 07 Signature d'un accord général de sécurité (AGS) avec la Principauté de Monaco

17 — 07 SGDSN — Remise au Premier Ministre du rapport d'étape sur la sécurité dans les transports

01 — 09
Diffusion de la posture vigipirate « Rentrée 2017 »

06 — 09

L'ouragan IRMA frappe Saint-Barthélemy et Saint-Martin

24 — 09

Elections sénatoriales

27 — 10
Diffusion de la posture Vigipirate « Transition 2017-2018 »

14-15 — 11
SGDSN
Exercice de réponse à une série d'attentats NRBC

08 — 12
SGDSN
Organisation d'une commission interministérielle de sûreté aérienne (CISA) sur la politique nationale de sûreté et de défense aérienne

21 — 12
Signature d'un accord général de sécurité (AGS) avec le Monténégro

05 — 09
Activation de la Cellule Interministérielle de Crise (CIC) pour l'ouragan IRMA

19 — 09
L'ouragan MARIA frappe la Guadeloupe

01 — 10
Attentat à la gare Saint-Charles de Marseille, deux victimes décédées

03 — 09
Essai nucléaire de la Corée du Nord

REVUE STRATÉGIQUE DE CYBERDÉFENSE : UN EXERCICE INÉDIT POUR LE SGDSN

Entrepris par le SGDSN sur la base d'un mandat confié par le Premier ministre le 21 juillet 2017, la *Revue stratégique de cyberdéfense* est le premier grand exercice de synthèse stratégique dans ce domaine. Véritable Livre blanc, cette *Revue* entend jeter les bases d'une ambition de cyberdéfense pour la France.

La *Revue stratégique de cyberdéfense* dont la version publique a été présentée le 12 février 2018 est l'aboutissement d'un important travail interministériel de réflexion et de consultation, mené sur six mois. Il s'appuie sur 200 auditions de personnalités françaises et étrangères, ainsi que sur la production de six groupes de travail et la réunion de vingt séminaires thématiques.

La *Revue* a fait l'objet d'un examen en Conseil de défense et de sécurité nationale et d'une communication en Conseil des ministres le 8 février 2018.

Organisée en trois parties, la *Revue stratégique de cyberdéfense* dresse un panorama de la cybermenace, formule des propositions d'amélioration de la cyberdéfense de la Nation et ouvre des perspectives visant à améliorer la cybersécurité de la société française.

1. La première partie de la *Revue* offre, pour la première fois dans une production officielle de l'administration française, une analyse globale des « dangers du monde cybernétique ».

Le paysage international apparaît caractérisé par le développement de capacités offensives, notamment par un petit nombre de puissances bien identifiées, et par un cadre de régulation encore incomplet, dont les fondements théoriques doivent encore être confortés ; la France, à cet égard, a manifesté son rejet du « hack back » et s'est engagée en faveur de la responsabilisation des États dans la lutte contre les cyberattaques fomentées depuis leur territoire.

2. Mettant en avant l'État comme responsable de la cyberdéfense de la Nation, la deuxième partie de la *Revue* s'attache à consolider le modèle français de cyberdéfense, fondé sur la séparation des fonctions offensives et défensives, ces dernières étant assurées, au premier chef, par l'ANSSI.

La *Revue* trace en outre le cadre doctrinal et d'organisation de la cyberdéfense française. Elle appelle à la mise en place de quatre chaînes opérationnelles pour remplir ces missions : protection, action militaire, renseignement et investigation judiciaire.

3. La troisième partie de la *Revue* met en avant le concept de souveraineté numérique, entendue comme le fait de conserver une capacité autonome d'appréciation, d'action et décision dans le domaine cybernétique, tout en protégeant d'autres composantes de la souveraineté nationale face aux nouvelles menaces engendrées par la numérisation. Cette souveraineté doit reposer, notamment, sur la maîtrise de certaines technologies telles que le chiffrement, et sur la consolidation d'une base industrielle nationale ou européenne.

L'État se pose ainsi en garant d'un niveau élevé de cybersécurité pour l'ensemble de la société.

La version publique de la Revue stratégique de cyberdéfense est disponible en libre téléchargement sur le site du SGDSN (www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense)

– COORDONNER & PILOTER

– LE CONTEXTE

Service du Premier ministre travaillant en liaison étroite avec la présidence de la République, le secrétariat général de la défense et de la sécurité nationale (SGDSN) assiste le chef du Gouvernement dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Il assure quatre missions principales :

- la préparation, le secrétariat et l'ampliation des décisions du Conseil de défense et de sécurité nationale (CDSN) ;
- la veille et l'alerte face aux menaces et aux risques, qui le conduisent à s'informer sur les situations de crise, à préparer les plans gouvernementaux et à assurer l'organisation de l'État en réponse à de telles situations ;
- le conseil au plus haut niveau de l'État en matière de défense et de sécurité nationale et l'élaboration des projets de loi et des textes réglementaires dans ses domaines de compétences ;
- des fonctions d'opérateur, principalement dans la gestion des habilitations de sécurité, des documents classifiés, des communications gouvernementales ou encore de la sécurité des systèmes d'information.

– 2017 : UNE ANNÉE DE TRANSITION

L'ANNÉE 2017 SE CARACTÉRISE PAR UN CYCLE D'ÉLECTIONS QUI A ENTRAÎNÉ UN PROFOND RENOUVELLEMENT AU SOMMET DE L'ÉTAT ET AU SEIN DES ASSEMBLÉES PARLEMENTAIRES

Dans ce contexte, le secrétariat général de la défense et de la sécurité nationale (SGDSN) a joué un rôle essentiel dans plusieurs domaines dont le bon déroulement de ces échéances, dans la transition intervenue après l'élection présidentielle et dans la continuité de la gestion des grandes fonctions régaliennes, au sein du domaine de la défense et de la sécurité nationale.

LE GARANT DE LA COORDINATION INTERMINISTÉRIELLE

Le SGDSN a la charge, au nom du Gouvernement, du traitement des sujets sensibles en matière de défense et de sécurité nationale. Son action recouvre, entre autres missions la coordination interministérielle à l'intérieur de son domaine de compétences, la planification de la gestion de crise, les transmissions gouvernementales sécurisées, la sécurité des systèmes d'information, la coordination de dossiers relatifs à des technologies sensibles et enfin, la coordination des enseignements de défense et de sécurité. Le SGDSN est aussi l'autorité nationale de sécurité, en charge de la réglementation relative au secret de la défense nationale.

Le SGDSN est sollicité pour proposer au Président de la République – chef des armées – et au Premier ministre – responsable de la Défense nationale et de l'administration- des réponses préparées avec les ministères compétents dans le domaine de la défense et de la sécurité nationale. Organiquement rattaché au Premier ministre, le SGDSN assure le secrétariat des Conseils de défense, mène des travaux d'anticipation stratégique et assure le suivi des crises internationales, au bénéfice du Conseil national du renseignement et de la lutte contre le terrorisme (CNRLT), par exemple.

LE GARDIEN DU PROCESSUS DÉMOCRATIQUE

L'année 2017 a été marquée par un fort renouvellement institutionnel, à l'occasion des élections présidentielle, législatives et sénatoriales.

Face aux risques d'une menace de déstabilisation démocratique et pour éviter tout doute quant à l'intégrité du scrutin, le SGDSN a, dès l'automne 2016, sensibilisé les candidats aux élections primaires organisées par les partis politiques. Pour ce faire, il a donné mission à l'ANSSI et à son centre des opérations de prendre les dispositions adéquates en amont et durant le processus électoral.

D'octobre 2016 à février 2017, le SGDSN et l'ANSSI ont engagé un travail visant successivement à évaluer la menace, informer et sensibiliser les partis politiques, les autorités et acteurs du processus électoral *via* des séminaires et à accompagner l'ensemble des parties prenantes dans la sécurisation des systèmes d'information concourant au processus électoral.

Le SGDSN a également été sollicité par des instances comme le Conseil constitutionnel et la Commission nationale de contrôle de l'élection présidentielle pour leur apporter un soutien dans le domaine de la cybersécurité et une expertise d'ensemble face à la menace émergente.

En lien avec la Commission nationale de contrôle de l'élection présidentielle et le Premier ministre, une procédure d'intervention de l'ANSSI a été formalisée. Désormais, il lui devenait possible de secourir un protagoniste de la campagne électorale en cas d'attaque sur ses systèmes d'information. Une telle intervention n'était toutefois envisageable qu'au cas où les dommages sur les systèmes d'information visés pouvaient avoir une incidence sur le déroulement de la campagne électorale ou remettre en cause l'équité entre les candidats.

(Voir aussi chapitre « Protéger et sécuriser» page 19)

42
CDSN

15 *JOURS*
ACTIVATION
de
LA **CIC**

4
POSTURES
VIGIPIRATE

2 EXERCICES
MAJEURS
+
+
+
+
PIRATE MER
mars
+
+
+
+
NRBC
novembre

4
PLANS
GOUVERNEMENTAUX
VALIDÉS

4
RAPPORTS
REMIS AU
1ER MINISTRE

42 CDSN EN 2017

Le Conseil de défense et de sécurité nationale (CDSN) a compétence sur toutes les questions de défense et de sécurité nationale : programmation militaire ou de sécurité intérieure, politique de dissuasion, sécurité économique et énergétique, lutte contre le terrorisme ou planification des réponses aux crises…

Le SGDSN en assure le secrétariat depuis 1906. Cette activité s'est notablement intensifiée depuis 2015, année au cours de laquelle le CDSN a été réuni à 10 reprises au lieu de deux ou trois habituellement. En 2016, 32 réunions ont été tenues et en 2017, il a été convoqué 42 fois. Le passage au rythme hebdomadaire, souhaité après l'attentat de Nice en juillet 2016, a été confirmé dès la prise de fonction du nouveau Président de la République, qui a choisi d'en faire un moment-clef d'examen de l'évolution des dossiers et de la prise de décision.

Le SGDSN, en s'appuyant sur des travaux interministériels conduits en amont, élabore pour chaque Conseil un dossier destiné au Président de la République, au Premier ministre, aux ministres présents et aux autres participants.

Ce dossier, au contenu très variable en fonction de l'ordre du jour et du vaste éventail des sujets possibles, comporte des analyses et des propositions d'arbitrage. Après la réunion, le SGDSN est également responsable de la préparation et de la diffusion du relevé de décisions signé par le Président de la République.

VIGIPIRATE : VERS LA SORTIE DE L'ÉTAT D'URGENCE

Quatre postures VIGIPIRATE ont été successivement adoptées en 2017 dont une pour assurer spécifiquement la sécurité de la période électorale. La dernière, « Transition 2017-2018 », a été diffusée le 27 octobre. Elle s'inscrit

dans le contexte de la sortie de l'état d'urgence et de l'adoption du projet de loi renforçant la sécurité intérieure et de lutte contre le terrorisme.

Cette posture actualise les mesures de vigilance et de protection pour faire face à la menace terroriste. Le dispositif de sécurité nationale s'est adapté pour tenir compte des vulnérabilités propres à la période de fin d'année 2017 et du début d'année 2018 (festivités et célébrations de fin d'année, période de soldes hivernaux, départs en vacances, etc.).

2 EXERCICES MAJEURS EN 2017, UN TROISIÈME EN PRÉPARATION

Le SGDSN est directement impliqué dans la préparation et la mise en œuvre des mesures de défense et de sécurité sur le territoire national. Ces mesures s'appuient notamment sur le travail de planification qu'il élabore en amont avec les différents ministères et qu'il fait évaluer par des exercices. Il s'appuie pour cela sur la direction de la protection et de la sécurité de l'État (PSE).

En 2017, deux exercices ont été joués. Un troisième, METROPIRATE, aurait dû avoir lieu au mois de décembre. Décalé de quelques semaines, il s'est tenu en janvier 2018. Tous les exercices ont pour objectif d'entraîner les chaînes de commandement interministérielle, ministérielles et locales ainsi que les unités d'intervention généralistes ou spécialisées.

Les 28 et 29 mars, l'exercice PIRATE-MER a permis la validation des nouvelles dispositions du plan dans l'hypothèse de réaction à un acte de piraterie, de brigandage ou de terrorisme en mer.

Les 14 et 15 novembre, le SGDSN a conduit un exercice d'application du plan NRBC (menace nucléaire, radiologique, biologique et chimique) ; il s'agissait de tester l'organisation de l'État face à un acte de terrorisme de ce type.

L'année 2017 aura également permis au SGDSN de valider quatre plans gouvernementaux pour adapter la réponse de l'État à l'évolution des risques et menaces : Crue de Seine, PIRANET, PIRATE-MER et PIRATAIR-INTRUSAIR. Dans son rôle de planification, le SGDSN a engagé la refonte et conduit la signature de l'instruction interministérielle IIM 10100, support de l'opération Sentinelle pour adapter la participation des armées à la protection du territoire et de la population.

SÉCURISER LES TRANSPORTS

Le SGDSN a reçu mandat du Premier ministre pour assurer la coordination de travaux interministériels qui ont permis la constitution d'un plan d'action pour le renforcement de la sécurité dans les transports. Ce plan comporte plusieurs axes autour de la connaissance de la menace, du renforcement des réseaux et infrastructures, de l'amélioration du contrôle des passagers, etc.

Afin de valider les avancées de la mise en place du plan, le SGDSN est chargé de la rédaction de rapports d'étapes transmis au cabinet du Premier ministre. Le dernier en date (juillet 2017) visait à optimiser la coordination et le pilotage politique des enjeux de sûreté des transports terrestres. Parmi les propositions soumises au Premier ministre figure la création d'une commission interministérielle de la sûreté des transports terrestres, inspirée des instances existantes du domaine aérien (commission interministérielle de la sûreté aérienne – CISA) et, plus récemment, du domaine maritime (commission interministérielle de la sûreté maritime et portuaire – CISMaP).

– FOCUS SUR...

PRÉALABLEMENT À SON APPROBATION, CHAQUE PLAN EST TESTÉ LORS D'EXERCICES DESTINÉS À MESURER LA PERTINENCE DES STRATÉGIES DE RÉPONSE GOUVERNEMENTALE MISES EN ŒUVRE.

***2017** AURA ÉTÉ MARQUÉ PAR DEUX EXERCICES :* ***PIRATE-MER 17 ET NRBC 17**.*

Dans le cadre de sa mission de prévention et de gestion des risques, le SGDSN organise ces exercices, dits « majeurs .» Ils permettent aux responsables gouvernementaux et territoriaux de s'approprier les nouvelles dispositions des plans à travers des scénarios de crise qui, par leur importance, conduisent à l'activation de la cellule interministérielle de crise (CIC) et des centres opérationnels zonaux et départementaux.

PIRATE-MER 17

PIRATE-MER est un plan gouvernemental de réponse en cas d'acte de terrorisme en mer, de piraterie et de brigandage. Son objectif est de décrire l'organisation de la gestion de crise et de préparer des stratégies de réponses à partir de situations de référence prédéterminées.

Les 28 et 29 mars 2017, le SGDSN a conduit l'exercice PIRATE-MER 17. Objectif : valider les dispositions du nouveau plan, avant sa diffusion en juillet.

La France est la seconde puissance maritime mondiale en superficie, avec quelque 11,5 millions de km² de zone économique exclusive (ZEE). Ce domaine maritime est d'une importance économique considérable ; l'économie de la mer représente ainsi plus de 14 % du PIB national (soit 270 milliards d'euros, et plus de 820 000 emplois).

Ce secteur crucial de l'économie n'est pas exempt de risques et de menaces, piraterie et terrorisme maritime en tête.

Le scénario du Plan PIRATE-MER 17 s'articulait autour d'une attaque perpétrée par un groupe terroriste sur un navire à passagers en mer.

NRBC 17

Validé en décembre 2016, le plan NRBC, qui s'appuie sur une importante coopération interministérielle, se veut un outil de référence pour les décideurs en situation de gestion de crise NRBC. Il comprend un guide d'aide à la décision qui prend en compte différents scénarios. Afin de former les acteurs ministériels à la gestion de crise et mettre à l'épreuve les recommandations du plan, des exercices sont organisés par le SGDSN dont le dernier en date, NRBC 17, a été conduit les 14 et 15 novembre 2017.

Le dispositif comprend un volet « prévention » fondé sur un corpus de textes et un volet « intervention » qui s'appuie notamment sur le plan gouvernemental. Le SGDSN a autorité pour conduire un programme interministériel de recherche et développement, qui traite de la connaissance des agents NRBC, de leur détection et du développement de contre-mesures médicales.

Enfin, le SGDSN préside le comité stratégique NRBC-E (E pour Explosifs) en charge du pilotage du dispositif national de réponse aux menaces terroristes NRBC-E. Dans le cadre de la coopération interministérielle, ce comité réunit sept ministères : intérieur, santé, défense, transports, agriculture, industrie, budget. Il s'appuie sur les laboratoires et les experts des domaines NRBC du SGDSN et de l'extérieur. ▲

LE CTG : GARANT DE LA SÉCURISATION DES TRANSMISSIONS

Pour assurer une partie de ses missions, le secrétaire général de la défense et de la sécurité nationale dispose, pour emploi et sous son autorité, d'une unité militaire interarmées dénommée centre de transmissions gouvernemental (CTG).

Parmi ses missions, le CTG :

- met en œuvre les transmissions sécurisées des plus hautes autorités de l'État ;
- exploite et soutient les systèmes d'information de l'état-major particulier (EMP) du Président de la République et du cabinet militaire du Premier ministre ;
- administre les moyens interministériels sécurisés de gestion de crise ;
- assure l'interfonctionnement des messageries formelles des ministères ;
- déploie et soutient les systèmes interministériels sécurisés conçus par l'ANSSI.

En 2017, l'installation du système de téléphonie fixe sécurisée OSIRIS auprès des cabinets du Président de la République, du Premier ministre et de plusieurs ministères a été un succès. Piloté par l'ANSSI en qualité de chef de projet, le nouveau système a permis d'accroître le volume de communications sécurisées en quelques mois.

En sus, le SGDSN a organisé deux réunions de la commission interministérielle de sûreté aérienne (CISA) le 4 juillet et le 8 décembre. La CISA a pour mission d'assister le Premier ministre dans le domaine de la politique nationale de sûreté et de défense aérienne.

C'est dans cette optique que le SGDSN a réalisé l'audit de 15 aéroports en 2017 au titre du programme « vols entrants .» Ce programme de coopération internationale vise à évaluer le niveau de sûreté des escales étrangères au sein desquelles les intérêts français sont en jeu. 19 audits supplémentaires sont programmés en 2018.

Enfin, dans la lutte contre la menace des missiles sol-air de très courte portée (SATCP), le SGDSN a évalué sept aéroports étrangers en 2017 et neuf en France. L'année 2018 verra la poursuite de ces évaluations tant sur le territoire national qu'à l'extérieur.

Toujours en juillet 2017, le SGDSN a également remis un rapport final relatif à la lutte contre les menaces asymétriques. Enfin, le 1er septembre, c'est un rapport consécutif au décret publié durant l'été par le Gouvernement sur la mise en place d'un fichier (ACCReD) qui a été déposé sur le bureau du Premier ministre.

CIC : 15 JOURS D'ACTIVATION POUR IRMA

La cellule interministérielle de crise (CIC) a été activée 15 jours en 2017 ce qui représente une nette baisse par rapport à l'année précédente (36), rejoignant un volume d'activation proche de la moyenne annuelle. Au total, le SGDSN a comptabilisé 100 jours d'activation depuis les attentats de janvier 2015 (dont 53 jours pour des crises réelles, hors exercice).

Le SGDSN a proposé au Premier ministre l'activation de la CIC le 5 septembre 2017 suite à l'arrivée du cyclone IRMA sur les îles du Nord des Antilles.
(Voir chapitre « Éclairer et Planifier » page 35).

STRUCTURER LA FILIÈRE INDUSTRIELLE DES TECHNOLOGIES DE SÉCURITÉ

Depuis 2013, le comité de la filière industrielle de sécurité (CoFIS) soutient l'activité des industries françaises sur ce marché concurrentiel mais en croissance constante.

Cette filière représente un chiffre d'affaires de 35 milliards d'euros, dont 21 pour le secteur industriel, et 300 000 emplois, dont 125 000 dans l'industrie selon les dernières évaluations.

Le secteur français des industries de sécurité figure parmi les meilleurs au niveau européen, réalisant environ 50 % de son chiffre d'affaires à l'exportation.

Dans cette optique de promotion de la compétitivité de la filière, deux actions importantes ont été lancées à l'automne 2017 : la mise en place d'un observatoire de la filière des industries de sécurité et la rédaction d'un document de politique industrielle mentionnant les principaux objectifs de la filière industrielle des technologies de sécurité à l'horizon 2025.

L'observatoire, porté par le Conseil des Industries de la Confiance et de la Sécurité (CICS) en partenariat avec le SGDSN, la direction générale des entreprises du ministère de l'économie (DGE), le délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces du ministère de l'intérieur (DMISC), le groupement

des industries de défense terrestres et aéroterrestres GICAT et le salon mondial de la sécurité intérieure MILIPOL, vise à développer un ensemble d'outils permettant le suivi de la filière *via* des analyses de marché, une recension des entreprises, l'évolution de divers indicateurs, etc. Les premiers résultats ont été présentés le 21 novembre dans le cadre du 20e salon Milipol à Paris.

OSIRIS : CRÉER LA CULTURE DE LA SÉCURITÉ POUR LES NOUVEAUX CABINETS

Afin de protéger la confidentialité du travail gouvernemental, le SGDSN a mandaté l'ANSSI pour concevoir des téléphones fixes permettant aux hautes autorités d'échanger des informations du niveau Confidentiel Défense, avec une échéance bien précise : la mise en place de la nouvelle équipe gouvernementale. Au printemps, l'ANSSI a entamé l'installation des nouveaux téléphones OSIRIS. À ce jour, le cabinet du Président de la République, celui du Premier ministre et ceux de neuf ministres ont été équipés. En 2018, l'installation de ce réseau se poursuivra au sein des autres cabinets ministériels, puis des services déconcentrés de l'État.

(Voir « Protéger et Sécuriser » page 19).

PRESCRIPTEUR ET DIFFUSEUR D'UNE CULTURE DE LA SÉCURITÉ

Dans le cadre de sa démarche de diffusion d'une culture de la sécurité au sein de la société, le SGDSN a diffusé de nombreuses publications (guides, recommandations, fiches pratiques, etc.) en 2017. Au total, en collaboration avec le service d'information du Gouvernement (SIG) et les ministères, 12 guides ont été élaborés à destination des exploitants et des personnels de certains types d'établissements, privés et publics, recevant du public, des organisateurs de grands événements et des collectivités territoriales.

Parmi les domaines et questions ayant donné lieu à sensibilisation, on peut citer :

- des recommandations pour la sécurisation des lieux de rassemblement ouverts au public (juillet) ;
- les méthodes de sécurisation d'un établissement face à la menace terroriste dans le cadre des Journées Européennes du Patrimoine (septembre) ;
- la sécurité numérique : l'hameçonnage (novembre) ;
- la circulation de produits chimiques : le signalement de tout vol ou utilisation suspecte (novembre).

Ce corpus vise à améliorer la prise de conscience face aux risques par la diffusion de messages spécifiques à l'ensemble des lieux et publics.

RENFORCER LA SÉCURITÉ DES OPÉRATEURS DE SERVICES ESSENTIELS

Malgré les recommandations de l'ANSSI, le niveau de cybersécurité des hébergeurs et prestataires informatiques progresse plus lentement que la menace. Leurs clients sont donc exposés à un risque majeur.

Le SGDSN préconise une approche ambitieuse de la transposition de la directive européenne sur la sécurité des réseaux et des systèmes d'information (directive *Network and Information Society* - NIS), qui prévoit d'imposer des obligations en matière de cybersécurité à des opérateurs fournissant des services essentiels pour le fonctionnement de l'économie et de la société, sur le modèle existant pour les opérateurs d'importance vitale.

3 Questions à ...

Philippe Decouais, chef de service de l'administration générale (SAG) au SGDSN

Quelles évolutions peut-on noter en termes de recrutement ? Voit-on apparaître de nouveaux profils ?

En 2012, le SGDSN employait quelque 500 personnes. En 2017, elles sont plus de 1100. L'un des enjeux du SAG est donc d'accompagner cette montée en puissance de nos effectifs.

Cette année, le besoin de recrutement le plus important émane de l'ANSSI, corollaire de l'élargissement de son périmètre d'intervention. Le constat que nous faisons dans le cadre de l'augmentation des effectifs de l'ANSSI est la difficulté à recruter des profils adaptés, principalement parce qu'on ne forme pas assez d'ingénieurs en France. Or, ces ingénieurs sont le profil-type des professionnels recherchés par l'agence.

À côté des femmes et hommes de terrain que sont les personnels militaires (au nombre de 300), le SGDSN a intégré des agents aux métiers très divers pour anticiper et répondre aux menaces diverses que nous tentons de prévenir : médecin, biologiste, vétérinaire… l'ensemble est une mosaïque de profils atypique qui requiert une certaine délicatesse dans sa gestion.

L'ANSSI aussi, au-delà de ses besoins en ingénieurs, rassemble une grande diversité de métiers : juristes, experts des questions européennes, mathématiciens de pointe ou spécialistes de la communication… Cette diversité est un phénomène assez nouveau. Il devrait prendre de l'ampleur à mesure que les missions de l'ANSSI croissent.

Le SGDSN et, particulièrement, l'ANSSI favorisent la mobilité et cherchent toujours de nouveaux profils. En quoi est-ce positif ?

L'aspect positif de ce renouvellement des personnels est qu'il nous maintient constamment à l'état de l'art grâce à l'embauche des meilleurs des jeunes diplômés ; autre bénéfice, une fois passés par l'ANSSI, ces personnels, formés et de haut niveau, rejoignent de grandes sociétés et peuvent y sensibiliser, former et entraîner à prévenir la cyber-menace, ce qui revient *de facto* à relever le niveau de cybersécurité de notre pays.

Au-delà de l'aspect recrutement, le SAG a également une mission d'ordonnateur des dépenses du SGDSN. Quels sont les grands chantiers de 2017 ?

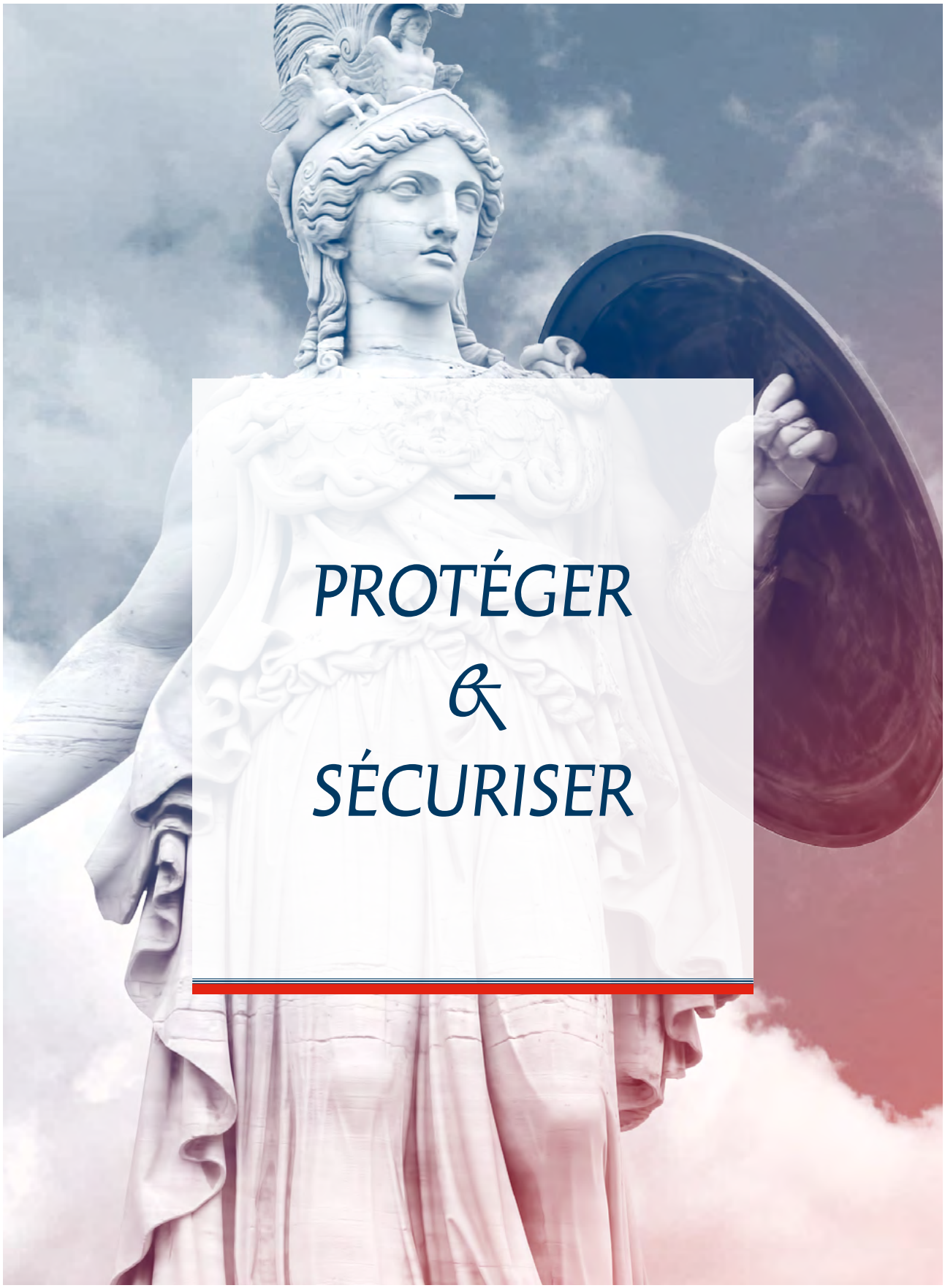
Le SAG agit en tant qu'autorité en matière d'investissement d'infrastructure. À ce titre, le principal projet en cours est la construction d'un centre de données à Rosny-sous-Bois pour l'ANSSI. Sur le site historique des Invalides, le SAG a procédé à de nombreux travaux de rénovation de l'infrastructure et d'amélioration des conditions de travail, à l'installation de nouvelles salles de serveurs informatiques et à l'aménagement de 135 nouveaux postes de travail complets. ▲

LE SGDSN AU CŒUR DE LA REVUE STRATÉGIQUE DE DÉFENSE ET DE SÉCURITÉ NATIONALE

La mise en cohérence des actions menées en matière de recherche scientifique et de projets technologiques intéressant la défense et la sécurité nationale est le cœur des missions du SGDSN. Afin d'assurer cette cohérence et la coordination des études prospectives menées par les différents ministères et la mise en œuvre des recommandations émises par le SGDSN, un Comité Interministériel de la Prospective (CIP) a été mis en place à l'automne 2015. Il est piloté par le SGDSN.

Par ailleurs, le SGDSN s'est impliqué dans la *Revue Stratégique de la Défense et de sécurité nationale 2017* conduite de juillet à décembre. Confiée par le Président de la République à la ministre des armées, cette *Revue* stratégique vise à tirer les leçons de l'évolution, depuis le Livre Blanc de la défense et de la sécurité nationale de 2013, d'un contexte stratégique aujourd'hui marqué par une menace terroriste durablement élevée. Cette *Revue* aura préparé l'élaboration de la loi de programmation militaire présentée le 8 février 2018.

Au cours de ce travail mené par le ministère des armées, sous la conduite de monsieur Arnaud Danjean, député européen, les directions du SGDSN ont été sollicitées. Le SGDSN y a dressé des perspectives concernant les défis à venir pour la sécurité nationale. Ce document de référence a décrit une méthode pour les années à venir consistant à porter une politique globale de soutien à l'innovation et à favoriser la transformation globale de l'écosystème militaire et industriel. Cet écosystème doit gagner en réactivité pour susciter, capter et intégrer les ruptures, technologiques ou d'usage issues du domaine civil. La *Revue Stratégique* propose d'une certaine manière d'étendre la « méthode agile » à l'ensemble des acteurs de la défense, afin de permettre aux forces françaises de conserver leur supériorité opérationnelle, face à des adversaires eux-mêmes inventifs et réactifs. ▲



PROTÉGER & SÉCURISER

– LE CONTEXTE

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est placée sous l'autorité du Premier ministre et rattachée au secrétaire général de la défense et de la sécurité nationale. Service à compétence nationale, l'agence peut intervenir sur tout le territoire national au profit de l'État et des opérateurs d'importance vitale (OIV).

Elle assiste le secrétaire général dans l'exercice de ses attributions en matière de sécurité des systèmes d'information et de moyens de commandement et de communications électroniques nécessaires aux plus hautes autorités en matière de défense et de sécurité nationale.

Elle est l'autorité nationale en matière de sécurité des systèmes d'information et, à ce titre, en matière de défense des systèmes d'information

Elle s'organise autour de plusieurs sous-directions :

- le centre opérationnel de la sécurité des systèmes d'information (COSSI) ;
- la sous-direction Expertise (SDE);
- la sous-direction systèmes d'information sécurisées (SIS) ;
- la sous-direction relations extérieures et coordination (RELEC).

– 2017 : UNE ANNÉE DE PRISE DE CONSCIENCE

Contre les tentatives de déstabilisation du processus démocratique ou les cyberattaques massives et répétées qui tentent de déstabiliser les États et les économies, le SGDSN dispose d'une pièce maîtresse : l'ANSSI. L'agence prévient et combat les cyberattaques, mais aussi inspire la doctrine nationale ou promeut les bonnes pratiques en matière de sécurité numérique. Un modèle français qui s'exporte.

L'ANSSI tient une place centrale dans la chaine de la défense et de la sécurité nationale pilotée par le SGDSN. Assurant la protection et la défense des systèmes d'information de ses bénéficiaires, elle ne mène ni cyberattaque, ni activité de renseignement, à la différence de certaines agences étrangères qui mêlent activités offensives et défensives. En revanche, l'ANSSI assure une fonction globale de prévention et de réaction aux cyberattaques, orientée vers les administrations, les OIV et bientôt les opérateurs de services essentiels (OSE).

DEUX CYBERATTAQUES MASSIVES

L'année 2017 a été marquée par les deux cyberattaques *WannaCry* et *NotPetya*, tout à la fois complexes, sophistiquées et dont les effets, importants, ont touché un nombre très important de systèmes et d'entreprises, sur un territoire très étendu. Ces attaques massives et aveugles ont toutes les deux exploité une faille de sécurité nommée *EternalBlue*.

La campagne d'attaques *WannaCry* survenue en mai 2017 a été conduite *via* un rançongiciel qui chiffre les données de ses victimes pour ensuite exiger une rançon, en échange de la clef de déchiffrement. *WannaCry* est considéré comme la plus importante attaque de cette nature connue à ce jour avec 300 000 ordinateurs infectés dans plus de 150 pays, principalement en Inde, aux États-Unis et en Russie.

La deuxième cyberattaque, *NotPetya*, est intervenue en juin 2017. Son *modus operandi* est légèrement différent de celui de *WannaCry* mais, surtout, sa finalité est toute autre : c'est le sabotage à grande échelle. *NotPetya* est un maliciel qui, une fois installé au sein d'un système d'information, se propage très rapidement jusqu'à de nouvelles cibles. À la différence d'un rançongiciel, son but est d'effacer les données des victimes.

L'autre particularité de *NotPetya* est que l'attaquant ne frappe pas directement ses victimes mais infecte un logiciel de comptabilité, nommé MeDOC, dont l'usage est obligatoire en Ukraine. Cela explique que *NotPetya* ait d'abord affecté l'ensemble des opérateurs et fonctions vitaux ou sensibles d'Ukraine parmi lesquels les services gouvernementaux, la distribution d'électricité, les banques, les télécommunications, les transports, la grande distribution et les médias, pour se propager ensuite dans plusieurs filiales ukrainiennes d'entreprises européennes.

Afin de riposter à ces attaques, l'ANSSI rappelle l'importance du cloisonnement, qu'il s'applique aux systèmes ou aux réseaux. Cette défense consiste notamment à cloisonner les systèmes d'information en fonction de leur objet ou de leur sensibilité aux attaques. De surcroît, le cloisonnement peut se faire sur un critère géographique afin d'éviter la propagation d'un virus à l'ensemble des systèmes d'information d'une entreprise présente dans de nombreuses pays.

12 OPÉRATIONS CYBERDÉFENSE

DONT **3** DÉBUTÉES EN **2016**

794 INCIDENTS

2435 SIGNALEMENTS

1621 traités

3 CRISES

1 GRAND ÉVÉNEMENT

ÉLECTIONS

LE COSSI AUX AVANT-POSTES

En réponse à ces nouvelles menaces, l'ANSSI a développé une approche transversale visant à anticiper par des audits, prévenir grâce à son expertise et réagir grâce à ses capacités d'information et de communication. La coordination des capacités et des effets recherchés implique un effort soutenu d'organisation interne et un dialogue permanent avec l'administration et les OIV.

Via son centre opérationnel, l'agence veille en permanence au bon état des systèmes d'information dont elle a la garde. Afin de contribuer à l'amélioration préventive de la sécurité des systèmes d'information, le COSSI réalise des audits de sécurité. En cas d'attaque, il a aussi la capacité d'intervenir auprès de la victime à des fins d'analyse et de reconstruction du système attaqué.

En 2017, le COSSI a réalisé 65 audits de sécurité de systèmes d'information auprès de ses bénéficiaires. Le nombre d'audits « à la demande » est en augmentation, passant de 60 à 65 % de la charge totale des prestations du COSSI.

DÉTECTER À PLUS GRANDE ÉCHELLE

Disposant de la signature des virus répertoriés et de marqueurs techniques rattachables à des attaques, les appareils de détection de l'ANSSI signalent le passage des données suspectes à l'entrée des systèmes protégés.

Au-delà de la fonction de vigie contre les attaques, ces équipements sont aussi les balises indispensables à l'établissement de la cartographie de la menace et une capacité de détection essentielle à la connaissance et l'anticipation de la menace que l'ANSSI améliore continûment.

En 2018, l'ANSSI franchira une étape supplémentaire dans le développement de ses capacités techniques avec l'entrée en service de son propre centre de données.

L'agence améliorera ainsi sa capacité d'analyse d'importants volumes d'informations et amplifiera sensiblement ses capacités de détection des cyberattaques.

DES VISAS DE SÉCURITÉ POUR INSTAURER UN ÉCOSYSTÈME DE CONFIANCE

Les « Visas de sécurité » délivrés par l'ANSSI sont un élément important dans la construction d'un écosystème de confiance.

Ces visas sont essentiellement de trois types distincts :

- la certification atteste de la robustesse d'un produit de sécurité. Elle est une boîte à outils permettant à divers donneurs d'ordres de définir leurs critères de sécurité et de faire vérifier par un tiers la satisfaction de ces critères ;
- la qualification par l'État vaut recommandation d'usage par l'ANSSI dans un contexte donné ; elle implique une certification du produit complétée par la vérification d'impératifs de sécurité et de confiance ;
- l'agrément est une décision réglementaire qui autorise l'utilisation d'une solution préalablement qualifiée au traitement d'informations classifiées.

Au-delà des seuls logiciels et matériels, l'ANSSI qualifie des prestataires de services de cybersécurité. Six catégories de services différents font l'objet d'un visa de sécurité, parmi lesquels la détection des incidents de sécurité, la réponse aux incidents de sécurité, l'audit de la sécurité des systèmes d'information et la prestation d'externalisation des données dans le nuage (*Cloud computing*).

Le cas particulier du visa de sécurité qualifiant des services d'« informatique en nuage » revêt une importance particulière. En effet, de nombreuses entreprises font l'objet de cyberattaques qui visent les données hébergées hors de chez elles.

Pour répondre à ce besoin particulier, l'ANSSI a mis en place un dispositif de qualification des prestataires d'informatique en nuage. Ces derniers se distingueront par le niveau élevé de sécurité avec lequel ils protègent les données qui leur sont confiées.

3 Questions à ...

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

En quoi 2017 est-elle une année charnière dans la prise de conscience du risque cybernétique ?

Des attaques comme WannaCry sont la concrétisation de craintes que nous avions et des scénarios que nous avions imaginés.

En 2017, nous avons découvert une nouvelle victime de cyberattaques : la démocratie ! Désormais, à l'aune de ce qu'il s'est passé lors des élections présidentielles, aux États-Unis et en France, nos démocraties – et pas uniquement nos économies, nos sociétés, nos administrations – doivent poursuivre leur développement numérique en prenant en compte un risque numérique qui n'existait pas jusque-là. C'est une grande leçon !

Comment parvenir à améliorer la prise de conscience du risque cybernétique et comment œuvrer, à l'intérieur et hors de nos frontières, pour en faire une réelle priorité ?

Nous sommes face à des attaquants extrêmement agiles qui vont s'engouffrer dans chaque faille de sécurité. Dans le cas d'une entreprise internationale bien protégée en France, ils attaqueront une filiale à l'étranger moins bien défendue, puis ils tireront le fil. Il y a donc une véritable nécessité à développer et améliorer globalement la cybersécurité en Europe et au-delà. La sécurité est un *continuum*.

Quels sont les moyens dont dispose le SGDSN pour anticiper, détecter les attaques et menaces cybernétiques ?

Ce qui est fondamental pour le SGDSN et l'ANSSI, c'est d'anticiper et identifier les menaces, de maîtriser la technologie, de comprendre les méthodes d'attaque, bien sûr, mais c'est aussi de fédérer l'ensemble des parties prenantes qui sont, aujourd'hui, multiples.

C'est pourquoi l'agence s'est constituée en pôle d'excellence et de référence. Pour ce faire, nous avons des laboratoires qui font aussi bien de la recherche ouverte que des travaux très poussés. Nous n'avons d'avenir que grâce à cette base technologique et scientifique de très haut niveau ; elle doit continuer de croître car les technologies mutent. De plus, il convient désormais d'enrichir nos travaux, par exemple en prenant mieux en compte les aspects de relations internationales ou les particularités économiques de chacun des grands secteurs d'activité avec lesquels nous interagissons. ▲

DES PUBLICATIONS ET FORMATIONS POUR CRÉER LA DOCTRINE

Face à des cybermenaces de plus en plus sophistiquées et variées, le SGDSN délègue à l'ANSSI le soin de produire la doctrine en matière de sécurité numérique. À ce titre, les sept laboratoires de recherche de l'agence ont publié en 2017 plus de cinquante articles scientifiques et ont participé à de nombreux colloques internationaux. L'ANSSI a également publié durant l'année écoulée une dizaine de guides pratiques et techniques.

En plus des formations courtes qu'elle propose aux agents de l'État et au personnel des OIV, l'agence a lancé en 2017 le label SecNumedu. Ce label répond à un cahier des charges destiné à valoriser les filières de l'enseignement supérieur et de la recherche qui forment à la sécurité numérique. SecNumedu vise à donner de la lisibilité à l'offre de formation ainsi qu'à de nouveaux métiers comme celui d'architecte des systèmes d'informations sécurisés. À ce jour, plus de 40 établissements de formation initiale et continue ont reçu cette certification.

L'ANSSI OUVRE LE CODE-SOURCE DE CLIP OS

Pour les besoins de ses travaux de recherche et le développement de plateformes de communications sécurisées, l'ANSSI a conçu depuis dix ans son propre système d'exploitation, Clip OS. Aujourd'hui, Clip OS est passé du stade de prototype à celui d'outil en service au sein de l'administration et de certains OIV.

Dans la continuité de sa mission de promotion et de partage des bonnes pratiques de sécurité numérique, l'ANSSI met maintenant progressivement à disposition de la communauté des développeurs le code-source de Clip OS. Cette action s'inscrit dans la logique de transparence et de modernisation numérique souhaitée par l'État, en vue d'instaurer un climat de confiance avec le citoyen.

SecNumacadémie : UN MOOC POUR UNE SÉCURITÉ NUMÉRIQUE AU QUOTIDIEN

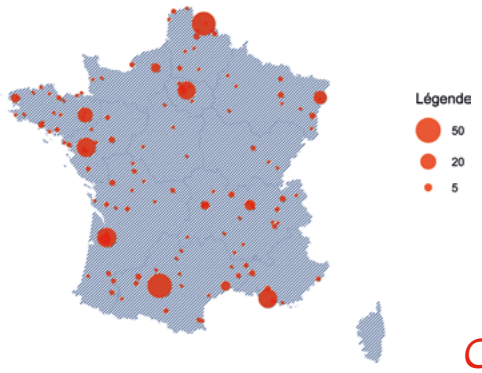
Lancée en mai 2017, cette formation en ligne (MOOC) a pour objectif de permettre aux étudiants, salariés, dirigeants d'entreprise ou particuliers d'être initiés à la cybersécurité ou d'approfondir leurs connaissances afin de pouvoir agir efficacement sur la sécurité de leurs systèmes d'information.

Un premier module a été mis en ligne le 18 mai. Le programme complet est constitué de quatre modules de formation qui ont été diffusés en septembre et décembre 2017- le 4e et dernier chapitre l'a été en février 2018.

Ce premier MOOC dont le programme et les contenus ont été créés par l'ANSSI est un succès puisque mi-décembre, la plate-forme comptait plus de 49 000 inscrits !

SecNum académie
ANSSI

Depuis son lancement le 17 octobre 2017, la plate-forme cybermalveillance.gouv.fr a enregistré 4 030 déclarations d'actes de cybermalveillance.



Nombre d'interventions réalisées par les délégués à la sécurité numérique en régions en 2017

L'ANSSI ÉLARGIT SON CHAMP D'ACTION

Dans le prolongement d'une réflexion interministérielle sur l'avenir de l'action territoriale en matière de sécurité numérique, l'ANSSI s'est dotée d'un dispositif d'action visant à soutenir le tissu économique et les institutions à l'échelle régionale.

En 2017, 11 délégués de l'ANSSI en régions, tous spécialistes de la sécurité numérique, ont œuvré avec les structures et les autorités régionales pour prévenir les incidents et sensibiliser les acteurs locaux du public et du privé aux bonnes pratiques informatiques.

Deux délégués supplémentaires seront désignés en 2018, afin de couvrir l'ensemble du territoire de la France métropolitaine.

CYBERMALVEILLANCE.GOUV.FR : S'ADRESSER À L'ENSEMBLE DES VICTIMES

Annoncé en 2016, cybermalveillance.gouv.fr est un projet interministériel incubé au sein de l'ANSSI et copiloté par le ministère de l'intérieur, avec l'appui des ministères de l'économie et des finances, de la justice et le secrétariat d'État chargé du numérique. Cette plateforme Internet d'assistance aux victimes d'actes de cybermalveillance est entrée en service le 17 octobre 2017.

Elle s'adresse aux particuliers, entreprises et collectivités territoriales… et remplit trois missions : la sensibilisation à la sécurité numérique, la mise en relation des victimes de cyberattaques avec des prestataires de proximité et l'animation d'un observatoire de la menace numérique.

L'ANSSI SÉCURISE LES COMMUNICATIONS FIXES ET MOBILES DE L'ÉTAT

En 2017, l'ANSSI a piloté deux projets d'envergure visant à sécuriser les communications de l'État : l'installation d'un nouveau système de télécommunication sécurisée fixe interministériel nommé OSIRIS et l'équipement à grande échelle de la gendarmerie et de la police nationales avec des terminaux mobiles SECDROID.

L'ANSSI a également apporté son soutien à la direction interministérielle du numérique et du système d'information de l'État (DINSIC) dans le cadre du projet « TMSi », qui a permis d'équiper au printemps 2017 l'ensemble des cabinets ministériels en smartphones sécurisés au niveau Diffusion Restreinte.

Secdroid est une adaptation du système d'exploitation Android. Il a été modifié par l'ANSSI pour assurer un niveau de confidentialité des échanges de données très supérieur à celui des téléphones commercialisés. Ce système d'exploitation est utilisé au sein du SGDSN, mais aussi au ministère de la justice et au ministère de l'intérieur via les programmes NeoGend et NeoPol. En 2017, 80 000 terminaux Secdroid ont ainsi été mis en service sur le territoire.

L'autre projet majeur conduit en 2017 par l'ANSSI est la mise en place du système de téléphonie fixe sécurisé OSIRIS. Sa vocation est d'offrir des outils de communication sécurisés modernes et ergonomiques aux hautes autorités et à leur entourage immédiat.

UN ENJEU RÉGLEMENTAIRE : LA DIRECTIVE NIS

Le 19 décembre 2017 a été entamé au Sénat l'examen du projet de loi transposant en droit national la directive *NIS*. La principale innovation du projet est la création d'un statut d' « opérateur de service essentiel » (OSE). Inspiré du statut des OIV, les OSE seront désignés parmi les opérateurs agissant dans des champs « essentiels » au bon fonctionnement de l'économie et de la société.

Ces OSE devront renforcer la sécurité des systèmes d'information essentiels qu'ils exploitent lorsque ceux-ci « offrent des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture des dits services .»

Les mesures ainsi prises sont destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne. En 2018, après l'adoption définitive du projet de loi, le travail se poursuivra avec la déclinaison réglementaire indispensable à l'application de la loi. L'ANSSI est chargée de ce travail, au nom du Premier ministre.

PROMOUVOIR LA CYBERSÉCURITÉ À L'ÉCHELLE INTERNATIONALE

Dans le cadre de sa mission de sensibilisation, l'ANSSI a coordonné plusieurs événements internationaux et multiplié en 2017 sa présence lors de rencontres professionnelles afin de promouvoir la cybersécurité. Au total, l'agence a participé à plus de 100 événements en France (conférences, colloques, évènements territoriaux, séminaires, forums) et 30 à l'étranger.

Les 6 et 7 avril, sous l'impulsion du secrétaire général de la défense et de la sécurité nationale, elle a organisé la conférence internationale « Construire la paix et la sécurité internationales de la société numérique » à l'Unesco. L'événement a rassemblé pendant deux jours des représentants de l'économie numérique, d'organisations internationales, d'ONG, des chercheurs et des diplomates venus du monde entier pour échanger sur les moyens de faire d'Internet un espace de paix et de sécurité où le droit international s'appliquerait.

Un séminaire juridique sera organisé à Paris en 2018 en vue de préparer la 2e édition de la conférence internationale en 2019.

COOPÉRER AVEC NOS ALLIÉS ET PARTENAIRES POUR PRÉVENIR LES CRISES CYBERNÉTIQUES

Les coopérations structurelles, techniques et opérationnelles dans le domaine cybernétique sont des instruments stratégiques concourant à consolider la sécurité nationale et notre influence.

Elles permettent d'élever le niveau général de la sécurité du cyberespace et d'en renforcer la stabilité par l'amélioration des capacités et de résilience de pays alliés et partenaires, ainsi que des organisations internationales auxquelles nous appartenons. Elles contribuent également à améliorer la capacité nationale à faire face à une crise cybernétique de dimension

internationale. Elles sont enfin un vecteur efficace pour promouvoir l'offre et l'expertise française en matière de cybersécurité, pour faire connaître l'organisation nationale française et pour maintenir notre pays à l'état de l'art.

Les partenaires européens et occidentaux, avec qui les échanges et les coopérations sont aujourd'hui approfondis et réguliers, demeurent des associés privilégiés de la France.

Certaines zones sont par ailleurs prioritaires comme l'Afrique subsaharienne, notamment les pays francophones, l'Afrique du Nord, ainsi que certains pays du Moyen-Orient et d'Asie du Sud et de l'Est.

En 2017, l'ANSSI a notamment signé un accord de coopération avec son homologue tunisien, l'Agence Nationale de Sécurité Informatique (ANSI), qui vise à renforcer le partage d'informations, d'expériences et de bonnes pratiques.

DÉSTABILISATION DÉMOCRATIQUE : UNE ANNÉE À HAUT RISQUE

L'année 2017 a été marquée par plusieurs échéances électorales qui ont nécessité l'intervention active de l'ANSSI. Au vu des incidents constatés lors de l'élection américaine en 2016, et dans la perspective de l'élection présidentielle de mai 2017, le SGDSN a fait le choix dès la fin 2016 d'organiser un séminaire de sensibilisation des acteurs du processus électoral.

Ce séminaire a permis à l'ANSSI de présenter l'état de la menace, un retour d'expérience sur les évènements survenus aux États-Unis et les enseignements à en tirer. Les bonnes pratiques de sécurité des systèmes d'information ont été rappelées et une liste de prestataires de confiance a été fournie.

COOPÉRATION À TOUS LES NIVEAUX

Dans la continuité du travail de sensibilisation mené auprès des protagonistes du processus électoral, l'ANSSI a coopéré avec les institutions et ministères en charge du contrôle et de l'organisation des élections.

Le travail a été particulièrement étroit avec la Commission nationale de contrôle de la campagne de l'élection présidentielle (CNCCEP), le Conseil constitutionnel, la Haute autorité pour la transparence de la vie politique, ainsi que le ministère de l'intérieur et le ministère des affaires étrangères qui est en charge de l'organisation des élections pour les Français résidant à l'étranger.

Un travail spécifique a été mené conjointement avec le Conseil constitutionnel afin de garantir que la publication par celui-ci de la liste des parrainages de chacun des candidats se fasse dans les conditions prévues et que la consolidation des résultats puisse se faire sans le moindre doute.

Autre innovation, sur proposition du SGDSN, l'ANSSI a été chargé par la CNCCEP et le Conseil constitutionnel d'assurer une veille des réseaux sociaux. Cette veille avait pour objectif de détecter au plus tôt les incidents affectant les systèmes informatiques des candidats mais aussi d'anticiper l'émergence de fausses nouvelles et de campagnes de désinformation.

Indépendamment de l'effort soutenu, et nouveau, consenti à l'occasion des élections, l'ANSSI a édité en avril le guide « Sécurité numérique – Bonnes pratiques et outils à l'usage des hautes autorités » remis aux nouvelles équipes gouvernementales. Concomitamment, des guides pédagogiques ont été publiés et diffusés aux parlementaires.

VOTE ÉLECTRONIQUE : LE SGDSN EN CONSEIL

Le 6 mars 2017, le Gouvernement a annoncé l'abandon du vote électronique, pour les Français de l'étranger, lors des élections législatives de juin. Cette décision a été prise sur la base de recommandations formulées par les experts de l'ANSSI, en tenant compte du niveau de menace cybernétique extrêmement élevé qui pouvait affecter le bon déroulement du vote électronique. Cet avis défavorable a été suivi par le ministère de l'Europe et des affaires étrangères.

Aujourd'hui, l'ANSSI continue d'accompagner le ministère dans la mise en place d'une future plateforme de vote électronique parfaitement sécurisée. ▲

CONTRÔLER & CERTIFIER

– LE CONTEXTE

La direction des affaires internationales, stratégiques et technologiques (AIST) est chargée des dossiers internationaux, sous un angle stratégique, des questions de non-prolifération et de contrôle des exportations de matériels de guerre. Elle intervient dans le processus de contrôle des exportations de technologies duales. Elle a sur ces différents dossiers un rôle d'analyse, d'expertise et de prospective. Elle veille à la protection du potentiel scientifique et technique de la Nation et participe à la protection et au développement des intérêts nationaux stratégiques de défense et de sécurité nationale.

Elle est chargée d'organiser la concertation interministérielle nécessaire au traitement de ces dossiers. Elle contribue à la préparation des réunions des conseils de défense et de sécurité nationale, dans leurs formations plénières et spécialisées et au suivi de l'exécution des décisions arrêtées par ces instances.

Elle s'organise autour de trois sous-directions :

- la sous-direction Affaires internationales ;
- la sous-direction non-Prolifération, sciences et technologies ;
- la sous-direction Exportation des matériels de guerre ;
- la cellule d'autorité responsable du service réglementé Galileo est également rattachée à la direction.

– CONTRIBUER À LA SÉCURITÉ INTERNATIONALE

2017 : UNE ANNÉE DE PROSPECTIVE

Dans un environnement international marqué par une grande incertitude stratégique et une évolution rapide des technologies affectant la sécurité et la défense, l'identification et l'analyse des situations de crise permettent de prévenir et de traiter les menaces contre notre sécurité nationale.

Le SGDSN assure au profit des plus hautes autorités de l'État, une mission de veille, d'alerte, de suivi et de prospective des crises et conflits internationaux. Il contribue ainsi au renforcement des capacités de connaissance et d'anticipation de l'État, en particulier à travers les synthèses du renseignement qu'il effectue sous l'égide de la coordination nationale du renseignement et de la lutte contre le terrorisme et l'éclaire sur les choix politiques en matière de technologies sensibles.

Il est également chargé de coordonner la réflexion interministérielle sur les évolutions stratégiques susceptibles d'affecter les intérêts de la France et de l'Union européenne en matière de prolifération, de désarmement et de maîtrise des armements ou de lutte contre les menaces globales liées aux flux illicites. Le SGDSN est enfin responsable de la sécurisation des usages gouvernementaux du programme spatial européen Galileo.

La publication en 2017 du rapport *Chocs futurs* a mis en relief la dimension prospective de sa capacité d'analyse.

ÉLABORER UNE SYNTHÈSE DU RENSEIGNEMENT

Dans le domaine du renseignement, le SGDSN intervient en amont des décisions et en appui de la coordination nationale du renseignement et de la lutte contre le terrorisme, à travers l'animation de groupes de travail qui réunissent la communauté du renseignement et l'élaboration de synthèses de renseignement au bénéfice des plus hautes autorités de l'État sur les principales menaces pour la sécurité nationale : terrorisme, trafics d'armes, zones de crise, activité des États proliférants en matière nucléaire, biologique et chimique, etc.

Le SGDSN diffuse ainsi périodiquement une évaluation de la menace terroriste qui permet d'adapter les postures Vigipirate.

FAIRE LA SYNTHÈSE DES POSITIONS FRANÇAISES SUR CERTAINS GRANDS ENJEUX DE SÉCURITÉ INTERNATIONALE

Le SGDSN, représenté par sa direction AIST, pilote des groupes de travail interministériels sur des thèmes intéressant la sécurité nationale et internationale, dans le cadre de mandats confiés par la présidence de la République ou le cabinet du Premier ministre. Il conduit ainsi des travaux sur la défense anti-missiles balistiques (DAMB), la dissémination des armes légères et de petit calibre et le suivi de l'accord sur les activités nucléaires iraniennes.

Il coordonne la position interministérielle française sur le sujet des menaces dites « hybrides », définies comme celles résultant de l'engagement combiné de mode opératoires non-militaires (cyberattaques, désinformation, déstabilisation politique, corruption) et militaires, caractérisées par une recherche d'ambiguïté et permettant de dérouter un adversaire étatique. Cette position permet d'alimenter les discussions sur le sujet dans les enceintes internationales (UE, OTAN…).

La direction anime également un groupe interministériel d'anticipation des crises, qui a pour mission de dresser des scénarios d'évolution et des recommandations articulant prévention et réaction. Elle peut être sollicitée pour mettre en place des groupes interministériels de travail consacrés à certains théâtres d'opérations ou à une question spécifique de sécurité internationale. Elle pilote notamment la « stratégie interministérielle sahélo-saharienne », qui vise à renforcer les capacités de souveraineté et de gouvernance des pays de la zone concernée.

ANTICIPER LES « CHOCS FUTURS »

Le SGDSN a réalisé en 2017 un grand travail prospectif qui s'est traduit par la publication d'un rapport intitulé *Chocs futurs : impact des transformations et ruptures technologiques sur l'environnement stratégique* .

Les différentes études mettent en exergue les tendances de fond comme les ruptures technologiques qui, par les mutations profondes qu'elles entraînent, risquent d'ébranler les équilibres internationaux actuels et peuvent avoir, à l'horizon 2030, un impact majeur sur l'environnement stratégique de notre pays.

L'émergence de la conflictualité dans le cybermonde ou la multiplication des acteurs dans l'espace extra-atmosphérique sont des évolutions déjà observables, qui devraient s'accentuer dans un avenir proche.

Le rapport anticipe les conséquences de ruptures technologiques majeures dans des domaines aussi variés que les missiles et vecteurs hypervéloces, la militarisation de l'espace, la biologie de synthèse ou les risques causés par la démocratisation des processus de fabrication additive ("impression 3D"), la transformation de la guerre par les neurosciences, l'intelligence artificielle et la révolution quantique.

À travers *Chocs futurs* le SGDSN propose à la communauté stratégique française une réflexion approfondie sur les enjeux à venir en matière de sécurité et de défense nationale, sous l'angle technologique, mais aussi juridique et éthique. Ce rapport a contribué à enrichir les débats menés au ministère des armées dans le cadre de la *Revue stratégique de défense et de sécurité nationale 2017.*

2 Questions à ...

Frédéric Journès, directeur des affaires internationales, stratégiques et technologiques (AIST)

En 2017, le SGDSN a publié un document prospectif intitulé Chocs Futurs. Quel en était l'objectif ?

À côté de son travail de synthèse et de consolidation dans le domaine du renseignement, le SGDSN a réalisé un travail de prospective, public, sur des sujets technologiques qu'il estime être particulièrement importants pour l'avenir, en matière de défense et de sécurité. Cette publication est une première. Elle illustre ce qu'est l'ADN du SGDSN : un mélange de cette méticulosité qui s'attache à la production de documents écrits et un très haut niveau d'expertise et de technicité dans des domaines complexes. Une seconde publication prospective est envisageable en 2018 sur des sujets plus sociétaux et éthiques.

Le SGDSN est très investi dans la politique nationale satellitaire. Y a-t-il eu des évolutions en 2017 ?

Le SGDSN est l' « autorité nationale responsable » du programme Galileo, en charge de la protection du signal public réglementé ; Galileo est le système de géolocalisation par satellite le plus précis au monde et son signal gouvernemental, le « PRS », est le mieux protégé contre le brouillage et le leurrage. Le régime des autorisations d'accès à ce signal gouvernemental sécurisé figure dans un projet de loi voté par le Sénat en décembre 2017 et qui devrait être adopté en 2018.

Au-delà, l'année 2017 marque un changement pour la France en matière de spatial. Nous devons désormais prendre en compte l'émergence du *New Space*, c'est-à-dire d'un nouvel écosystème de l'industrie spatiale. La multiplication et la diversification des acteurs du domaine génèrent une croissance exponentielle des données désormais disponibles. La capacité de traitement des *Big data* a et aura une importance stratégique pour les États, les acteurs économiques et les individus. Le SGDSN a été sollicité pour apporter son expertise sur ces évolutions et sur les éventuelles réponses à élaborer : coordination des initiatives industrielles, du soutien éventuel de l'État, action de l'Union européenne, place des programmes préexistants... Il nous faut aussi protéger ces nouveaux savoir-faire et repenser notre approche du contrôle tout comme de la sécurité de nos systèmes satellitaires. ▲

CONTRÔLER LES DONNÉES SÉCURISÉES DE GALILEO

Dans le domaine spatial, le SGDSN pilote la commission interministérielle des données d'origine spatiale (CIDOS), qui assure le contrôle de diffusion des images spatiales par les opérateurs industriels. Les travaux réalisés en 2017 ont permis de mettre à jour la liste des restrictions, qui sera soumise à la validation de la commission.

Le SGDSN assure également la synthèse des positions nationales sur les questions de sécurité des programmes européens de navigation par satellite comme Galileo ou Egnos et de surveillance de la Terre comme Copernicus. S'agissant de Galileo, Ariane 5 a mis sur orbite en décembre 2017 quatre nouveaux satellites de communication qui complètent désormais la constellation Galileo. Ces satellites européens constituent un dispositif complet qui permet une géolocalisation contrôlée par des moyens techniques européens – contrairement à ceux qui existent déjà comme GPS, Glonass ou Beidu. Au sein du programme satellitaire Galileo, le SGDSN agit comme autorité nationale responsable de la sécurité des signaux protégés (*Public Regulated Service*).

La maîtrise de la sécurité de Galileo s'effectue en relation permanente avec les autres administrations nationales, la Commission européenne et les États membres du programme et sa coordination est donc assurée par le SGDSN du fait du caractère transverse de cette mission.

Le SGDSN assure également la synthèse des positions nationales sur les questions de sécurité des programmes européens de navigation par satellite

ENTRE ....

1ER

JANVIER

LA

CIEEMG

EXAMINE

6 000

demandes

de

LICENCE

ou

MODIFICATION

D'EXPORTATION

MATÉRIELS DE GUERRE

289

demandes

DISCUTÉES à la

CIEEMG

ET

31

DÉCEMBRE

CONTRÔLER LES EXPORTATIONS DE MATÉRIELS DE GUERRE

Contrôler les exportations d'armement et veiller sur le transfert des technologies sensibles ou encore lutter contre le risque de prolifération sont des missions fondamentales de contrôle et de certification du SGDSN. Le SGDSN joue un rôle d'animateur et de coordonnateur interministériel du dispositif national de lutte contre la prolifération en assurant la coordination de la réponse nationale.

La base de la politique d'exportation est le régime de prohibition *a priori*. Aucune exportation de matériels de guerre ne peut se faire sans une autorisation spécifique. L'octroi de ces autorisations, les licences d'exportation, relève de l'autorité du Premier ministre, et par délégation du SGDSN.

Une concertation interministérielle au sein de la CIEEMG (commission interministérielle pour l'étude de l'exportation des matériels de guerre) composée des ministères des armées, de l'Europe et des affaires étrangères, de l'économie et des finances permet d'étudier notamment les contraintes liées à notre souveraineté, à la protection de nos forces et à celle de nos alliés, au respect de nos engagements internationaux et aux enjeux industriels et économiques.

En dehors du traitement en flux continu des demandes de licence, des séances plénières de la CIEEMG sont organisées mensuellement pour traiter les dossiers les plus sensibles qui sont éventuellement arbitrés au niveau du cabinet du Premier ministre.

Un contrôle de la bonne exécution de l'exportation s'exerce au travers d'un nouveau dispositif de contrôle *a posteriori* du ministère des armées responsabilisant les entreprises exportatrices. Une volonté de transparence nationale et à l'égard de nos partenaires internationaux.

Dans un souci de transparence, un rapport annuel au Parlement français sur les exportations d'armement de la France est publié. Il est unique en Europe et est le seul instrument de ce type à fournir des informations aussi complètes sur les exportations réellement effectuées par le pays (prises de commandes et livraisons effectuées).

LES TRANSFERTS INTRACOMMUNAUTAIRES : L'INDISPENSABLE HARMONISATION COMMUNAUTAIRE POUR STRUCTURER LA BITDE

Dans le cadre de la *Letter of Intent* (*LoI*), le SGDSN anime et coordonne l'action du sous-comité *Export Control* lequel travaille à la fluidification des transferts d'armement entre les États parties (Allemagne, Espagne, France, Italie, Royaume-Uni et Suède). Les États parties de la *LoI* orientent et impulsent des actions multilatérales en vue de développer un cadre légal et réglementaire propice à la structuration et au développement de la base industrielle et technologique de défense européenne (BITDE) au niveau de l'Union européenne dans son ensemble.

Le SGDSN représente la France à la Commission européenne dans le cadre de la mise en œuvre de la directive Transferts intracommunautaires (2009/43/CE) et promeut la fluidification des transferts de matériels de guerre entre les États membres de l'Union européenne. À cette fin, le SGDSN coordonne l'action interministérielle française et œuvre au renforcement des licences générales de transfert à destination des entreprises certifiées, des forces armées, dans le cadre d'opérations de réparation et de maintenance et de présentation, d'évaluation et de démonstration.

Depuis 2016, le SGDSN conduit une action normative au niveau communautaire en défendant l'adoption de lignes directrices harmonisées sur la notion de « spécialement conçu pour un usage militaire ».

LE NÉCESSAIRE CONTRÔLE DES TECHNOLOGIES SENSIBLES

Le SGDSN assure aussi un encadrement plus spécifique des exportations et des ventes de technologies particulièrement sensibles comme le nucléaire civil et les satellites. Ainsi, en 2017, le SGDSN a poursuivi l'accompagnement des opérations commerciales dans le nucléaire avec la Chine et, en décembre 2017, il a été sollicité pour encadrer plusieurs exportations de satellites d'observation.

De manière plus générale se pose la question des équipements et technologies susceptibles d'être utilisés à des fins militaires ou pouvant participer au développement, à la production, ou au fonctionnement d'armes de destruction massive. Ces biens sensibles, qualifiés de biens à double usage (BDU), 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.

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 participe 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*. Il assure également l'instruction des dossiers sensibles pour le compte de la commission interministérielle des biens à double usage (CIBDU).

DIALOGUE SUR L'ESPACE ENTRE LA FRANCE ET LE JAPON

La deuxième session du dialogue global sur l'espace, destiné à accroître et renforcer les coopérations bilatérales relatives aux questions spatiales, s'est tenue le 24 mars 2017 à Tokyo. Co-présidé par le SGDSN pour la France et par le ministère des affaires étrangères et le secrétariat pour la politique spatiale nationale (NSPS), pour le Japon, ce dialogue a réuni les représentants des ministères et des agences responsables de l'espace des deux pays.

L'organisation de ce dialogue permet de donner une cohérence d'ensemble à la relation bilatérale dans le domaine de l'espace extra-atmosphérique et de développer de nouveaux domaines de coopération. Cette session du dialogue a permis de concrétiser la coopération bilatérale par la signature de deux documents :

- une Lettre d'Intention établissant le cadre du partenariat global franco-japonais sur l'espace et affirmant la volonté des parties d'explorer l'ensemble des domaines ouverts à la coopération en matière spatiale ;
- un arrangement technique établissant le cadre des échanges agréés en matière de surveillance de l'espace (*Space Situational Awareness-SSA*).

LUTTER CONTRE LA PROLIFÉRATION DES ARMES DE DESTRUCTION MASSIVE

La prolifération des armes de destruction massive menace directement la paix et la sécurité internationales l'empêcher est une des priorités de la politique étrangère et de défense française.

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 AIST assure une veille permanente dans les domaines concernés : nucléaire, radiologique, biologique, chimique, explosifs, missiles et spatial. Elle coordonne les études sur 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 interrompre, sous le pilotage opérationnel des services du SGDSN, les flux proliférants partout dans le monde et quels que soient leurs modes de transport.

PROTÉGER LE POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION

La compétitivité, la notoriété et l'excellence d'un établissement de recherche reposent notamment sur sa capacité d'innovation, ainsi que sur le développement et l'entretien de ses savoirs et savoir-faire. Le SGDSN est chargé du déploiement d'un dispositif de protection du potentiel scientifique et technique de la Nation (PPST) dont le but est de protéger, au sein des établissements de recherche publics et privés, ces savoirs et savoir-faire stratégiques ainsi que les technologies sensibles qui concourent aux intérêts souverains de la Nation. Il répond également à la double nécessité de ne pas entraver la recherche et de promouvoir l'indispensable rayonnement national et international des établissements.

Ce dispositif offre une protection juridique et administrative fondée sur le contrôle des accès aux informations stratégiques ou sensibles détenues. Les services compétents des ministères de tutelle des établissements participent à ces contrôles qui concourent activement à la prévention des risques de captation et de détournement.

Le SGDSN a un rôle d'animateur et de coordonnateur interministériel dans le dispositif national mis en place pour lutter contre la prolifération

– FOCUS SUR...

LE SGDSN AU CŒUR DE LA SÉCURITÉ DE L'ACCORD FRANCO-AUSTRALIEN DE COOPÉRATION

En avril 2016, la société DCNS (aujourd'hui Naval Group) a été retenue par le gouvernement australien pour participer à la construction de douze sous-marins océaniques, pour un budget total estimé à 34 milliards d'euros.

Ce programme de coopération entre la France et l'Australie s'étale sur une cinquantaine d'années, le premier des sous-marins devant entrer en service actif autour de 2030.

Les deux gouvernements sont étroitement associés dans l'encadrement de l'opération qui dépasse le seul cadre industriel. Un accord général de sécurité a été signé le 7 décembre 2016 pour régir les échanges d'informations classifiées et un accord intergouvernemental en date du 20 décembre de la même année organisent l'accompagnement de l'État. En mars 2017, la France et l'Australie ont « rehaussé » leur partenariat stratégique, marquant ainsi leur ambition d'approfondir leur coopération dans les domaines les plus sensibles.

À son niveau, le SGDSN est engagé dans cette démarche depuis son origine : en qualité d'autorité nationale de sécurité, il a négocié l'accord général de sécurité ; par ailleurs, il veille à la sécurité du programme dans sa durée, avec l'appui des services de l'État concernés. À cette fin, il co-anime un groupe de travail bilatéral, reflet du haut niveau de confiance que cette coopération implique.

Cette coopération inédite oblige également chacun des partenaires à adapter sa culture. Des personnels australiens et français vont résider pendant des mois, voire des années, sur les territoires respectifs des deux partenaires, afin de coopérer à la construction de ces sous-marins. Les Australiens par exemple n'ont jamais eu l'occasion dans le passé de sécuriser une infrastructure industrielle comme la France le fait autour de la fabrication de ses équipements de dissuasion nucléaire.

Tout au long de cette coopération, le sujet de la cybersécurité sera au cœur des préoccupations. Le SGDSN se prépare à la difficulté particulière que représente une gestion dans la durée de ce type de risques.

Au-delà du cadre industriel, l'accord implique une véritable intimité stratégique entre les deux pays qui ouvre un nouveau chapitre de la relation bilatérale entre la France et l'Australie. ▲

ÉCLAIRER & PLANIFIER

– LE CONTEXTE

La direction de la protection et de la sécurité de l'État (PSE) assiste le secrétaire général pour l'exercice de ses attributions relatives à la sécurité de l'État et à la protection des ressortissants et des intérêts français, sur le territoire national et à l'étranger, contre les menaces telles que le terrorisme et les risques majeurs. À ce titre, PSE est responsable de la préparation et de l'organisation de l'État face aux crises majeures qui peuvent affecter la continuité de son fonctionnement. Cette responsabilité s'exerce dans le cadre d'une approche multirisque, incluant les crises d'origine :

- naturelle ;
- industrielle ;
- terroriste ;
- ou au sein d'une coopération renforcée avec des partenaires européens et internationaux.

Pour couvrir l'ensemble de son action, la direction s'appuie sur une cinquantaine de cadres (militaires, policiers, gendarmes, administrateurs civils, experts de haut niveau, médecin, vétérinaire, ingénieurs,etc.), répartis au sein de :

- la sous-direction de la planification de sécurité nationale ;
- la sous-direction de la protection du secret de la défense nationale ;
- le pôle de développement des technologies de sécurité.

– 2017 : UN RISQUE TERRORISTE ÉLEVÉ ET PERSISTANT

DE NOUVEAU EN 2017, L'ACTIVITÉ DU SGDSN A ÉTÉ CONDITIONNÉE PAR LA PERSISTANCE DES MENACES TERRORISTE ET ISLAMISTE TRÈS ÉLEVÉES, NÉCESSITANT UNE FORTE MOBILISATION.

4 POSTURES VIGIPIRATE EN 2017

En fonction de l'évaluation de la menace terroriste, le SGDSN propose au Premier ministre une posture VIGIPIRATE qui comprend un ensemble de mesures et précautions à prendre, en vue de protéger nos concitoyens. Chaque posture est déclinée par les ministères, services déconcentrés de l'État et les opérateurs, dans leur champ de compétences.

En 2017, quatre postures ont été successivement tenues. Une posture particulière a été adoptée pour permettre la mise en sécurité des élections présidentielle et législatives. Une autre a pris en compte les particularités de la rentrée des classes. La dernière posture de l'année a été conçue pour prendre en compte les déplacements et les concentrations de populations des fêtes de fin d'année.

DES PLANS PIRATE EN CONSTANTE ADAPTATION

L'existence de menaces susceptibles d'affecter la continuité de l'État, la sécurité de la population, du territoire et des activités économiques et sociales impose de disposer d'un mécanisme gouvernemental de préparation et de réponse aux crises.

Les plans d'intervention de la famille PIRATE prévoient des réponses adaptées aux situations de crise graves comme les prises d'otages, les attentats ou les attaques biologiques, par exemple. Pour chaque scénario de crise, le SGDSN prépare les réponses à apporter et prévoit l'organisation des chaînes de commandement qui vont du sommet de l'État jusqu'au niveau le plus opérationnel, *via* les services déconcentrés des préfectures.

Ces outils de réponse à la crise sont constamment adaptés, afin de prendre en compte les évolutions de la menace. Toute crise intervenant dans un pays proche est étudiée avec l'ensemble des acteurs nationaux qui interviendraient face à une crise comparable. Les conclusions qui sont tirées de ces études entraînent des adaptations des plans.

Au mois de septembre 2017 a été publiée la nouvelle version du plan PIRANET. Ce plan, rénové par un travail commun conduit par l'ANSSI et PSE, vise à limiter les effets d'une cyberattaque en précisant le rôle de chacun des acteurs impliqués, en organisant la coordination d'ensemble, en adaptant spécifiquement le travail de la cellule interministérielle de crise à ce type de situation et en formalisant l'information des hautes autorités, aux fins de décision.

4 POSTURES **VIGIPIRATE** *en* 2017

—

5/09 2017 ACTIVATION *de la* **CIC** *pour* + + + + **IRMA**

—

15 AÉROPORTS AUDITÉS

—

41 AGS SIGNÉS À CE JOUR

—

2 AGS SIGNÉS *en* 017

Cette rénovation a conclu un travail engagé très en amont et partiellement validé grâce au succès d'un exercice organisé en décembre 2016. Les enseignements tirés de cet exercice ont été intégrés dans la version finale du plan. L'année 2017 a aussi permis de valider le plan PIRATE-MER grâce à un exercice organisé les 28 et 29 mars. Car en plus de l'adaptation permanente des plans, la professionnalisation des acteurs de la gestion de crise constitue un axe d'effort continu.

Les exercices permettent de créer et d'améliorer des habitudes de travail, sous tension, entre les acteurs de la gestion de crise. Face à l'événement, cette expérience commune permet de répondre de façon plus pertinente, plus rapide et plus efficace. Elle garantit aussi la capacité à maintenir l'effort dans la durée.

L'ANIMATION DU TRAVAIL INTERMINISTÉRIEL

Le SGDSN a remis trois rapports au Premier Ministre portant sur des aspects particuliers de la lutte anti-terroriste. Deux de ces rapports concernent la sécurité dans les transports, notamment les gares et les aéroports. Ils tirent les enseignements de divers évènements, dont certains graves, survenus à l'étranger.

Le troisième rapport dresse une liste de contre-mesures susceptibles d'être déployées face à des menaces dites « asymétriques », c'est-à-dire utilisant des moyens de circonstance ou atypiques. Dans ce cadre, le SGDSN a contribué à la mise au point d'un nouveau plan « NRBC » (menaces Nucléaires, Radiologiques, Biologiques, Chimiques) permettant de faire face à des situations nécessitant un traitement particulier

IRMA : LE SGDSN SUR LE FRONT DES CATASTROPHES NATURELLES

La cellule interministérielle de crise (CIC) a été activée par le Premier Ministre le 5 septembre 2017 pour répondre aux conséquences du passage du cyclone IRMA dans les Antilles. Le SGDSN est alors intervenu en appui du ministère de l'intérieur pour coordonner l'action des différents ministères et services déconcentrés de l'État.

Outre le ministère de l'intérieur, ont été mobilisés le ministère des outre-mer, le ministère des armées, le ministère des transports, de la transition énergétique et solidaire et le ministère de la santé et des solidarités. Des moyens de la zone de défense et de sécurité des Antilles, renforcés par des moyens métropolitains, ont été déployés. Les formations du service militaire adapté ont été mises à contribution d'emblée.

Dans le domaine des transports, PSE contribue au développement de doctrines

Des militaires de la sécurité civile ont été projetés sur place. Le ministère de l'Europe et des affaires étrangères a également été engagé pour assurer l'information des ressortissants résidant dans les autres pays de la zone et des touristes français susceptibles de s'y trouver.

Considérée initialement comme pouvant être traitée à l'échelon d'un ou deux ministères, IRMA s'est avérée devoir l'être en mobilisant un grand nombre d'acteurs. L'étendue des dégâts provoqués et la complexité des problèmes à résoudre ont nécessité une prise en compte interministérielle, par exemple pour mettre en place un pont aérien et une liaison maritime spécifique avec les Antilles.

DIALOGUE NATIONAL DE SÉCURITÉ : ÉLEVER LE NIVEAU DE CONSCIENCE

Le SGDSN agit également par des actions de diffusion d'informations auprès des forces vives de la Nation, via le Dialogue National de Sécurité. Ces informations s'adressent aux responsables de grands ensembles commerciaux, des salles de spectacle, des musées ainsi qu'au du monde de l'éducation. Dans ce domaine particulier, le SGDSN s'adresse aussi bien aux directeurs académiques des services de l'éducation nationale chargés d'animer et de mettre en œuvre la politique éducative dans les départements que, plus directement, aux chefs d'établissements.

L'objectif est de diffuser aussi largement que possible les bons réflexes de sécurité. Ce travail de longue haleine vise à élever le niveau de conscience de la population et à l'éduquer aux réflexes de sécurité.

Dans le domaine des transports, PSE contribue au développement d'une doctrine d'emploi des unités cynotechniques au contact des explosifs, militaires ou artisanaux. À titre expérimental, PSE collabore à la création d'un système de détection d'armes longues au travers de portiques.

2017 a vu également se poursuivre le travail engagé par le SGDSN, en collaboration avec la direction générale de l'aviation civile et le ministère de l'intérieur, autour de l'usage des drones – qu'ils soient considérés comme malveillants, non coopératifs malveillants ou coopératifs mais avec des comportements inappropriés.

COFIS : LA FILIÈRE DES INDUSTRIES DE SÉCURITÉ À L'HORIZON 2020

Depuis 2013, le CoFIS a pour mission d'accompagner l'élaboration et la mise en œuvre d'une stratégie nationale pour la filière des industries de sécurité. Un comité de pilotage, présidé par le SGDSN et rassemblant grands industriels, petites et moyennes entreprises, mais aussi les *start-up* du domaine, anime le travail de réflexion sur ce sujet. Le CoFIS est un remarquable exemple de coopération entre l'administration et les acteurs économiques et industriels privés.

Depuis 2015, l'Observatoire de la filière mène un travail d'identification des technologies « critiques » et les technologies de rupture nécessaires à la constitution ou la préservation d'une forme de souveraineté nationale dans ce domaine.

Le SGDSN soutient des programmes de recherche et de développement (« R&D »), sous-traités à des tiers de confiance, visant à développer des expérimentations correspondant aux menaces présentes et futures, effectives et potentielles. Ce travail dans le domaine de la « R&D » inclut des industriels, le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) et des opérateurs, comme des laboratoires spécialisés dans la manipulation d'agents pathogènes biologiques dangereux. Les résultats dégagés par ces recherches permettent d'adapter les politiques de prévention de la menace et les mesures de réponse aux crises.

DES PARTENARIATS INTERNATIONAUX ET DES COOPÉRATIONS RENFORCÉS

Le SGDSN a contracté de longue date des partenariats dans le domaine de la protection et de la sécurité de l'État avec les États-Unis, l'Allemagne ou la Grande-Bretagne. Ces coopérations passent par des d'échanges d'information et des partages d'expérience. La prévention contre la radicalisation est un axe de travail important. Il donne lieu à des travaux au rythme soutenu. En 2017, ces travaux ont été partagés avec les Pays-Bas, la Suède ou la Belgique, qui souhaitaient bénéficier de l'expertise française.

Le SGDSN travaille conjointement avec Julian King, le commissaire pour l'Union européenne de la sécurité, à la mise en œuvre du programme européen en matière de sécurité. Ce programme sur cinq ans vise à lutter contre le terrorisme, le crime organisé et la cybercriminalité. Le SGDSN développe des projets inspirés des initiatives françaises dans ces domaines.

DE NOUVEAUX ACCORDS GÉNÉRAUX DE SÉCURITÉ

Le SGDSN est autorité nationale de sécurité et, à ce titre, chargé de garantir la protection du secret de la défense nationale.

La direction de la protection et de la sécurité de l'État a pour missions de classifier les documents sensibles. Elle est le référent national en matière de réglementation et elle est le point de contact des autorités internationales, de l'Union Européenne et de l'OTAN.

En 2017, deux accords généraux de sécurité (AGS) ont été signés avec Monaco et le Monténégro. Au total 41 AGS sont aujourd'hui signés par la France.

À ce jour, des accords généraux de sécurité (AGS) ont été signés avec une quarantaine d'états. L'année 2017 a permis la rénovation de ces accords avec la Belgique et la Norvège, principalement sur les aspects numériques. Elle a vu enfin la signature d'un nouvel accord avec la Principauté de Monaco en juin et, avec le Monténégro, 29e pays à intégrer l'OTAN en décembre 2017. ▲

3 Questions à ...

Pascal Bolot, directeur de la protection et de la sécurité de l'État (PSE)

Quelle a été l'activité du SGDSN en matière d'évaluation des risques et de préparation des réponses opérationnelles ?

L'année 2017 s'inscrit dans la continuité de 2015 et 2016, avec d'une part un niveau très élevé des menaces terroriste et djihadiste et d'autre part avec une forte mobilisation du personnel en charge de la prévention et de la réponse aux menaces.

En 2017, quatre postures VIGIPIRATE distinctes ont été adoptées : la première en début d'année, puis une posture spécifique pour assurer la sécurité et le bon déroulement des élections présidentielle et législatives, une troisième au mois de septembre pour sécuriser la rentrée des classes et, enfin, une dernière posture au mois de décembre, afin de prendre en compte les rassemblements occasionnés par les fêtes de fin d'année.

La planification de sécurité nationale est une mission importante du SGDSN. Que recouvre-t-elle ?

Les plans d'intervention PIRATAIR et PIRATEMER constituent des réponses adaptées à des situations de crise de référence comme la prise d'otages, les tueries de masse, les attaques biologiques, etc. Pour chaque cas de figure théorique, nous fournissons des réponses et des solutions à chaque niveau de la chaîne de commandement, des plus hautes instances de l'État jusqu'au niveau le plus opérationnel, *via* les services déconcentrés des préfectures.

En collaboration avec l'ANSSI, le SGDSN a remis à plat le plan PIRANET qui vise à contrecarrer une menace cybernétique en prenant en compte les nouvelles dispositions, les retours d'expérience des attaques réelles ou des exercices mis en place tout au long de l'année. Ces documents de référence que sont les plans sont constamment adaptés par le SGDSN, compte tenu de l'évolution rapide des menaces.

Le SGDSN est-il également présent sur le front des catastrophes naturelles ?

Oui. La CIC a été activée par le Premier ministre le 5 septembre 2017 pour faire face aux conséquences du passage d'IRMA dans les Antilles. Le SGDSN est intervenu en appui du ministère de l'intérieur pour coordonner l'action des différents ministères et des services déconcentrés de l'État. Actuellement, nous rédigeons les circulaires relatives à l'organisation des chaînes de commandement de l' « arbre de décision .»

Si, au départ, IRMA était une crise « sectorielle », nous nous sommes rapidement rendu compte, au regard des dégâts, que de nombreux ministères étaient concernés. C'est tout l'intérêt de la CIC, cellule placée sous l'autorité du Premier ministre, que de pouvoir coordonner une réponse globale à un évènement de grande ampleur.

Dans ce cadre, le SGDSN a apporté son appui à la CIC pour coordonner l'action des différents ministères et des services déconcentrés de l'État. Les enseignements tirés de cette crise, conjugués aux retours d'expériences des crises de ces dernières années nous conduisent à réviser la circulaire du Premier ministre relative à l'organisation gouvernementale pour la gestion des crises majeures et à améliorer notre dispositif de veille et d'alerte ▲

– PSE : DES EXPERTS DE HAUT NIVEAU, DES COMPÉTENCES MUTUALISÉES, UNE PLANIFICATION DE POINTE

Pour couvrir l'ensemble de son action, la direction s'appuie sur une cinquantaine de personnels de statuts divers (militaires des armées, policiers, gendarmes, administrateurs civils, experts de haut niveau, médecin, vétérinaire, ingénieurs, etc.).

Cette diversité des profils est nécessaire face à la diversité des menaces et des crises. Ces experts maîtrisent l'état de l'art de leurs domaines de compétence respectifs mais sont également aptes à échanger avec leurs homologues étrangers, afin de partager l'information et la connaissance. Ils sont également à même de synthétiser les travaux de recherche publiés dans les domaines sensibles. Ces travaux inspirent ensuite des inflexions de la planification de sécurité nationale.

« Ils représentent l'interface entre le monde scientifique et administratif et ont vocation à appuyer la génération d'une bonne planification », résume Pascal Bolot.

51, boulevard de la Tour-Maubourg
75700 Paris cedex 07 SP

www.sgdsn.gouv.fr