AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANTICIPER

RAPPORT D'ACTIVITÉ 2015

ACCOMPAGNER

AGIR

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN

Édité par l'Agence nationale de la sécurité des systèmes d'information (ANSSI)
Directeur de la publication : Guillaume Poupard
Coordination : Laurent Célérier
Conception et réalisation : PCA / Vincent Treppoz
Crédits photos : Picturetank (Patrick Gaillardin, Patrice Normand, Florence Joubert) - CAYI - Istock - WikiCommons - DR
Impression : Direction de l'information légale et administrative (DILA)
Juillet 2016

Conseiller-maître à la Cour des comptes, Louis Gautier est le secrétaire général de la défense et de la sécurité nationale depuis octobre 2014.

Les technologies numériques sont désormais centrales dans notre vie quotidienne. Elles innervent nos outils de production, les services auxquels nous recourons, nos loisirs, mais aussi nos équipements de défense et nos systèmes d'importance vitale.

Ces technologies procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens.

Entre menace virtuelle et dommages matériels, la frontière s'est effectivement de plus en plus estompée, comme l'attestent l'usage malveillant des outils numériques et certaines attaques informatiques auxquelles nous sommes désormais possiblement exposés.

Cette imbrication croissante donne tout son sens au rattachement de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) au secrétariat général de la défense et de la sécurité nationale (SGDSN). Chargé d'assister le Premier ministre et le chef de l'État dans l'exercice de leurs responsabilités institutionnelles respectives en matière de sécurité et de défense, le SGDSN a pour principale mission de penser notre protection de manière globale, hors de tout cloisonnement institutionnel et de toute approche sectorielle exclusive. Principale gardienne des systèmes informatiques de l'État et des opérateurs d'importance vitale, l'ANSSI contribue à la poursuite de cet objectif en mettant son expertise numérique au service d'une approche inclusive de la sécurité et de la défense de nos concitoyens.

De cet apport et du rôle de l'agence au cœur du SGDSN et de notre dispositif national de défense, ce premier rapport d'activité est le reflet. Il témoigne de l'impératif catégorique qui est le nôtre : face à des adversaires toujours enclins à innover et à se jouer des frontières, géographiques, techniques ou intellectuelles, adapter et renforcer constamment notre réponse.

LA CYBERSÉCURITÉ EST PLUS QUE JAMAIS L'AFFAIRE DE TOUS ET DE CHACUN

Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), Guillaume Poupard tire les conclusions d'une année qui a mis l'agence sur le devant de la scène et vu l'adoption d'une stratégie nationale pour la sécurité du numérique.

QUELS SONT LES AXES STRATÉGIQUES QUI CARACTÉRISENT L'ACTION DE L'ANSSI ?

Au sein du SGDSN, l'ANSSI est là pour accompagner et sécuriser le développement du numérique. C'est une mission essentielle, face aux diverses menaces qui se développent en même temps que le numérique monte en charge dans la société, dans l'économie et dans notre vie quotidienne. La confiance dans le numérique – dont l'agence est l'un des garants – devient ainsi une priorité nationale et internationale. Au même titre que les avancées technologiques, c'est la sécurité qui permet la transformation numérique. La sécurité numérique implique un grand nombre d'acteurs, bien au-delà des seuls experts : les pouvoirs publics, les entreprises du secteur, tous les acteurs économiques, mais aussi les particuliers. Elle concerne en effet chacun d'entre nous, et seuls une attention et un effort collectifs peuvent garantir aujourd'hui la cybersécurité.

DANS CE CONTEXTE, COMMENT DÉFINIRIEZ-VOUS L'ANSSI ?

L'ANSSI est une agence située au cœur de l'État et au service de la nation, responsable des questions de sécurité numérique et informatique. Notre rôle est de comprendre et d'analyser les menaces, de les contrer et d'être un acteur majeur de la stratégie nationale de cybersécurité. Si je devais raisonner en termes de valeurs pour caractériser l'ANSSI, je dirais que les principales sont la compétence, l'agilité et l'ouverture.

QUELS ONT ÉTÉ LES PRINCIPAUX TEMPS FORTS DE 2015 ?

L'agence s'est beaucoup investie dans la protection des opérateurs d'importance vitale. Elle a d'ailleurs contribué, en 2015, à plusieurs textes d'application issus de la dernière loi de programmation militaire. De façon plus large, nous sommes fortement engagés dans la coconstruction de règles de cybersécurité. Toujours au titre de 2015, il faut bien sûr citer la présentation par le Premier ministre, le 16 octobre, de la Stratégie nationale pour la sécurité du numérique, fruit de travaux interministériels coordonnés par l'ANSSI. Il s'agit d'une réponse collective et coordonnée, afin de faire face à des pratiques criminelles, délictuelles ou déloyales, comme la cybercriminalité, l'espionnage, la propagande, le sabotage ou l'exploitation excessive de données personnelles.

Enfin, je citerais aussi l'affaire de TV5 Monde, première concrétisation – du moins visible par tous – de la volonté de détruire un acteur français. Au demeurant, nous avions anticipé le scénario global et cela a permis de rétablir rapidement la situation et, plus encore, d'en tirer des leçons pour l'avenir.

L'ANSSI FAIT FACE À D'IMPORTANTS BESOINS DE RECRUTEMENT…

Effectivement, nous sommes confrontés à un double phénomène. D'une part, le développement de nos missions et de nos interventions se traduit par un renforcement des effectifs de l'agence, d'où un besoin de recrutement. D'autre part, nous recrutons des talents qui acquièrent, au sein de l'agence, une expérience et un savoir-faire très appréciés chez les opérateurs. Nous avons donc un *turn-over* important. Mais cet essaimage de talents est avant tout un point positif pour le développement de la culture de la sécurité numérique.

QUE DIRIEZ-VOUS À UN JEUNE INFORMATICIEN POUR LE CONVAINCRE DE REJOINDRE L'ANSSI ?

On traite au sein de l'agence des choses qu'il ne verra jamais ailleurs et qui lui donneront une expérience sans équivalent. Le passage par l'ANSSI est, en quelque sorte, un exhausteur de carrière, avec un véritable enrichissement professionnel et des opportunités de formation continue. L'environnement de travail est à la fois jeune et dynamique – avec 25 % de moins de 30 ans et 40 % entre 30 et 40 ans – et les différents domaines couverts par l'agence sont suffisamment larges pour permettre des mobilités internes. Du côté des candidats, nous attendons – outre les compétences techniques – un véritable sens de la mission.

PEUT-ON DONNER QUELQUES EXEMPLES D'INTERVENTIONS ASSURÉES PAR DES PERSONNELS DE L'AGENCE ?

L'ANSSI fait appel à une grande diversité de métiers et de compétences : technologies high-tech, électronique, mathématiques, organisation, analyse du risque, relations internationales… L'agence mène aussi un important travail de sensibilisation et de prévention auprès des acteurs économiques, qu'ils soient publics ou privés. Nous développons également des produits de confiance avec le secteur privé. C'est le cas, par exemple, sur les moyens de chiffrement ou bien de détection et de traitement des attaques informatiques. Il faut savoir que la France a connu, en 2015, une vingtaine d'attaques majeures que je ne peux pas citer pour des raisons de sécurité, à l'exception de celle – très médiatisée – de TV5 Monde… Autre exemple : l'ANSSI a ouvert, en 2015, un chantier sur les objets connectés, sources d'innovation mais aussi de nouvelles menaces.

COMMENT L'ANSSI VA-T-ELLE ÉVOLUER DANS LES PROCHAINES ANNÉES ?

Elle va rester au cœur des missions de l'État. Avec la montée de la dimension numérique dans tous les aspects de l'économie et de la société, la place et les missions de l'ANSSI sont nécessairement vouées à s'accroître. L'agence va donc continuer à renforcer ses moyens, son expertise et ses relations avec les différents acteurs. Mais cela ne doit pas conduire à une déresponsabilisation de ces derniers. Il faut bien comprendre que la cybersécurité est, plus que jamais, l'affaire de tous et de chacun.

AU SERVICE DE LA sécurité informat

Agence nationale de la sécurité des systèmes d'information, l'ANSSI déploie des actions à destination des administrations et services publics, des entreprises ainsi que des particuliers. Elle développe également une recherche de pointe. Elle participe enfin à la définition de la politique nationale en matière de cybersécurité, et contribue à sa promotion dans les débats internationaux.

BÂTIR UN CADRE D'ACTION ADAPTÉ

Pour répondre aux attentes des acteurs publics et privés, la sécurité des systèmes d'information doit évoluer avec l'apparition de nouvelles technologies et de nouveaux usages. L'ANSSI met donc son expertise au service de l'élaboration de la réglementation française, européenne et internationale. Elle collabore également avec les États volontaires et s'implique au sein d'instances internationales. Enfin, elle travaille en lien avec les opérateurs français pour adapter ses actions à leurs besoins et relayer ses messages en région.

SENSIBILISER, FORMER ET ASSISTER

La sécurité des systèmes d'information relève, à des degrés divers, de la responsabilité de chacun. L'ANSSI mène donc des actions auprès de nombreux publics, afin de développer une culture de la sécurité numérique. Elle contribue ainsi au développement et à la certification de solutions informatiques de confiance. Elle apporte également conseil et assistance aux ministères, aux administrations, aux opérateurs d'importance vitale (OIV) et aux entreprises. Elle assure des audits des systèmes d'information des services de l'État et des OIV. Enfin, elle mène une politique de formation intensive et sensibilise le grand public grâce à des opérations de communication.

L'ANSSI EN 2015, CE SONT...

Près de **460 agents**.

108 agents engagés.

75 % de **contractuels**.

65 % d'agents de **moins de 40 ans**.

1 150 candidats ayant visionné les offres d'emploi en ligne de l'ANSSI.

528 actions de formation à destination du personnel de l'ANSSI.

266 bénéficiaires de formation au sein de l'ANSSI.

1 450 stagiaires externes à l'ANSSI accueillis pour des formations courtes dans le domaine de la cybersécurité.

ique

DÉVELOPPER DES OUTILS DE POINTE

Pour rester à l'avant-garde de la sécurité des systèmes d'information, il est indispensable d'anticiper les évolutions informatiques et de créer les outils pour y répondre ou les accompagner. L'ANSSI mène donc des travaux de recherche de haut niveau, reconnus en France et dans le monde entier. Elle développe également des systèmes d'information et de communication sécurisés pour le gouvernement.

DÉTECTER LES ATTAQUES ET Y RÉPONDRE

En cas d'attaque des systèmes d'information des administrations et des OIV, il est important d'agir vite. L'ANSSI offre donc un dispositif de détection aux services ministériels. Elle suit quotidiennement l'actualité mondiale en matière de sécurité des systèmes d'information et analyse vulnérabilités, risques et menaces. Elle a également déployé un service de réception de signalements d'incidents, ouvert 24 heures sur 24. Enfin, elle adapte sa réponse à l'ampleur de l'attaque et peut mettre en place une organisation de crise, si nécessaire.

UN PRESTIGIEUX HÉRITAGE

Créée par un décret du 7 juillet 2009, l'ANSSI remplace la Direction centrale de la sécurité des systèmes d'information (DCSSI). Si on remonte l'arbre généalogique de l'agence, composé d'institutions chargées de la sécurité des informations sensibles de l'Etat, on aboutit à la création, en 1943, à Alger, de la Direction technique du chiffre.

Plus de **20 ETP** consacrés à la recherche.

40 publications de recherche, sur des sujets aussi variés que la cryptographie, la reconnaissance vocale ou même les consoles de jeu.

96 produits certifiés.

350 rencontres bilatérales entre l'agence et les entreprises françaises de la cybersécurité, à des fins de cartographie et d'identification des besoins.

Plus de **2 300** codes malveillants collectés.

4 000 signalements reçus, soit 50 % de plus qu'en 2014.

Une vingtaine d'incidents majeurs de sécurité traités.

568 avis sur des correctifs de sécurité.

15 alertes sur des vulnérabilités critiques.

202 réunions internationales.

Des relations avec plus de **30 pays.**

120 interventions de sensibilisation.

63 interviews pour la presse papier et en ligne, ainsi que la radio.

8 616 abonnés au fil Twitter de l'ANSSI, @ANSSI_FR.

23 reportages pour la télévision.

L'ANSSI en 2015

JANVIER

7-9
Attentats en région parisienne. À cette occasion, l'ANSSI active son dispositif de crise.

20-21
Participation de l'ANSSI à la septième édition du Forum international de la cybersécurité (FIC), à Lille.
La feuille de route du plan Cybersécurité de la Nouvelle France industrielle, piloté par Guillaume Poupard, directeur de l'ANSSI, est rendue publique.

FÉVRIER

20
Mise en ligne du nouveau site Internet de l'ANSSI, plus intuitif et plus convivial, dans le cadre d'une politique de communication ambitieuse.

MARS

24
Publication par l'ANSSI et la Confédération générale des petites et moyennes entreprises (CGPME) du *Guide des bonnes pratiques de l'informatique.*

Crash du vol 9525 de la compagnie German Wings dans le sud de la France. À cette occasion, l'ANSSI active son dispositif de crise.

29
Publication de trois décrets d'application de la loi de programmation militaire (LPM) 2014-2019, relatifs à la sécurité des systèmes d'information. Ces textes représentent une nouvelle étape d'un processus législatif dans lequel l'ANSSI s'est particulièrement investie.

AVRIL

8
Début de l'attaque contre TV5 Monde. L'ANSSI est mobilisée dès les premières minutes. Son intervention, en collaboration avec les équipes de la chaîne, prend fin en juillet.

MAI

7
Signature d'une convention entre l'ANSSI et l'Union des groupements d'achats publics (UGAP), pour mieux faire connaître les produits et prestations labellisés par l'ANSSI et en faciliter l'achat par les collectivités publiques.

18
Lancement de la seconde phase de la Nouvelle France industrielle (NFI). L'ANSSI assure la codirection du plan Confiance numérique de cette stratégie, dédié au développement des acteurs du secteur de la cybersécurité et à la promotion des exportations en la matière.

JUIN

2-4

Participation de l'ANSSI au salon Infosecurity Europe, au sein du pavillon français. Cette manifestation réunit les acteurs de la cybersécurité du monde entier.

20

L'ANSSI est présente à la nuit du Hack.

JUILLET

7

Co-organisation par l'ANSSI d'une journée de conférences à l'occasion de la Cloud Week, qui se déroule du 6 au 10 juillet à Paris, en présence du BSI, l'homologue allemand de l'agence.

SEPTEMBRE

CyberEdu
La sécurité par l'enseignement supérieur des NTIC

30

Mise à disposition de documents pédagogiques « clés en main » sur la cybersécurité à destination des enseignants en informatique, dans le cadre du projet CyberEdu, initié en 2014 par l'ANSSI.

OCTOBRE

3

Du 30 septembre au 3 octobre, participation de l'ANSSI aux 15e Assises de la sécurité et des systèmes d'information, à Monaco. Dans son discours d'ouverture, Guillaume Poupard, directeur général de l'agence, salue la mise en place progressive d'une cyberdéfense ambitieuse pour la France.

16

Présentation par le Premier ministre de la Stratégie nationale pour la sécurité du numérique, résultat de travaux interministériels coordonnés par l'ANSSI.

21

Intervention de l'ANSSI aux 3e Rencontres parlementaires de la cybersécurité, organisées à l'École militaire.

NOVEMBRE

24

Lancement de la campagne #CyberVigilant. Elle rappelle les bonnes pratiques de sécurité et encourage la mise en place de mesures de précautions simples.

30

Du 30 novembre au 11 décembre, tenue de la COP21 à Paris. À cette occasion, l'ANSSI active son dispositif de crise.

DÉCEMBRE

4

Début du déploiement du réseau des référents ANSSI en régions, pour toucher les acteurs locaux.

8

Approbation de la directive européenne Network & Information Security (NIS), au terme d'un processus auquel l'ANSSI a beaucoup contribué. La reprise de la philosophie de la loi de programmation militaire (LPM) 2014-2019 traduit le succès de la vision française de la cybersécurité.

CYBER EUROPE enisa CYBER EUROPE

À LA RESCOUSSE de TV5 Monde

Le 8 avril 2015, aux alentours de 21 heures, les comptes Twitter et la page Facebook de TV5 Monde se mettent à diffuser des messages de propagande à la gloire de l'État islamique, puis les émissions de la chaîne cessent. Le début d'une course contre la montre pour les équipes de l'ANSSI, sollicitée dès les premières minutes de l'attaque.

L'inquiétude a vite succédé à la surprise, chez TV5 Monde, le 8 avril, quand les comptes Twitter et la page Facebook de la chaîne francophone internationale se sont mis aux couleurs du Cybercaliphate, un groupe de pirates se revendiquant de Daech.

Les dégâts ne se sont cependant pas arrêtés là : quelques minutes plus tard, la page d'accueil du site Internet de TV5 Monde est à son tour défigurée et la diffusion de la chaîne cesse. De plus, sa messagerie professionnelle est hors d'usage, tout comme une bonne partie de son système d'information. Avant que les équipes techniques de TV5 Monde débranchent tout, pour limiter les dégâts, les attaquants ont même effacé les micrologiciels, des codes installés lors de la construction du matériel informatique et sans lesquels il ne peut fonctionner. L'attaque a donc été perpétrée à des fins de sabotage – une première en France.

REPRENDRE LE CONTRÔLE DU SYSTÈME D'INFORMATION

Contactée dans les premières minutes de l'incident, l'ANSSI est immédiatement intervenue, bien que TV5 Monde ne soit pas un opérateur d'importance vitale (OIV). Les premiers jours, jusqu'à vingt agents de l'agence ont travaillé aux côtés des équipes techniques de la chaîne pour reconstruire et sécuriser le système d'information endommagé. Dans un premier temps, elles ont mené en parallèle une activité de cartographie, pour mieux connaître le périmètre défendu, et des investigations, en veillant à préserver les preuves. Puis, elles ont repris le contrôle du système d'information, tout en élevant son niveau de sécurité, afin d'éviter tout retour des assaillants. Les programmes ont repris le 9 avril, petit à petit. À 5 heures, un programme unique a été diffusé sur tous les canaux.
Vers 10 heures, chaque chaîne a renoué avec ses propres séquences. Enfin, à 18 heures, le journal, en direct, s'est déroulé de manière normale. Cependant, l'intervention de l'ANSSI n'était pas achevée. Ses équipes ont été mobilisées jusqu'à la fin du mois de juillet, afin de gérer la prise de relais par des prestataires de confiance privés.

DES VERTUS PÉDAGOGIQUES

L'enquête a révélé que les attaquants se sont introduits dans le système d'information de TV5 Monde plusieurs semaines avant l'attaque. Cependant, TV5 Monde avait fait le choix d'une sécurité limitée, ayant pour priorité la disponibilité de son système d'information. La chaîne a d'ailleurs reconnu un défaut d'anticipation de la menace, lors d'une intervention devant d'autres dirigeants de l'audiovisuel, le 27 avril. Ce témoignage, écouté avec beaucoup d'attention, a permis de relayer les préoccupations de sécurité numérique auprès de ce secteur et a eu des vertus préventives certaines.

UNE STRATÉGIE pour l'avenir

Le 16 octobre, le Premier ministre a rendu publique la Stratégie nationale pour la sécurité du numérique, née de travaux interministériels coordonnés par l'ANSSI. Ce document doit accompagner la transition numérique de la société française et, grâce à une réponse collective en cinq axes, favoriser la stabilité de l'État, le développement économique et la protection des citoyens.

La numérisation de la société française progresse à grands pas. Porteuse d'innovation et de croissance, elle concernera, à terme, la quasi-totalité des produits, services et métiers. Or, des pratiques criminelles, délictueuses ou déloyales mettent à mal la confiance et la sécurité des usagers. Pour répondre aux enjeux et aux menaces nés de la transition numérique, une action coordonnée est indispensable.

PROTÉGER

La Stratégie nationale pour la sécurité du numérique offre un cadre au développement de la cybersécurité. Son premier axe concerne les infrastructures et opérateurs essentiels. La stratégie affirme la nécessité de garantir leur sécurité numérique et, ainsi, la souveraineté de la France. Pour ce faire, elle prévoit notamment de mettre en place une réglementation renforcée et un groupe d'experts pour la confiance numérique chargé d'identifier les besoins et les technologies-clés.

La Stratégie nationale se penche par ailleurs sur la protection de la vie numérique, la lutte contre la cybercriminalité et l'assistance aux victimes. Parmi les mesures retenues figure notamment le lancement d'un dispositif national dédié aux victimes de cybermalveillance.

DÉVELOPPER ET SENSIBILISER

Le troisième axe de la Stratégie nationale aborde, quant à lui, l'information des citoyens. Entre autres mesures, les formations initiales et continues comporteront un volet « sécurité numérique » adapté, pour favoriser les comportements responsables dans le cyberespace. La stratégie affirme ensuite la volonté de faire de la sécurité numérique un facteur de compétitivité, en aidant les entreprises françaises à proposer des produits et des services de haut niveau. Pour ce faire, l'État s'engage à soutenir la recherche, l'innovation et les exportations dans le domaine de la cybersécurité.

UNIR TOUTES LES FORCES

Le dernier axe de la stratégie s'intéresse à la place de la France dans l'espace cyber international. Il a pour ambition de la renforcer, via, notamment, une autonomie numérique stratégique des pays volontaires de l'Union européenne et la promotion d'un cyberespace sûr et ouvert. Il est, par exemple, proposé de fournir un soutien capacitaire en matière de cybersécurité aux pays qui le souhaitent.

UNE MISE EN ŒUVRE PROGRESSIVE

Comme tous les acteurs concernés, dont les ministères, l'ANSSI doit contribuer à la mise en œuvre de la Stratégie nationale pour la sécurité du numérique, en fonction de ses attributions. L'agence a déjà commencé ce travail en publiant, dès le 8 février 2016, sa stratégie « ANSSI 2020 ». Cette feuille de route, qui ne couvre pas l'ensemble des activités de l'agence, décline et complète le document national. Elle sera mise en œuvre progressivement et actualisée chaque année.

ANTICIPER

En matière de sécurité des systèmes d'information, adapter sa posture à un environnement en perpétuelle évolution est une obligation. C'est pour répondre à cette exigence que l'ANSSI s'est dotée d'un département de recherche agile et performant lui assurant une grande visibilité sur les derniers développements technologiques. Elle veille également à suivre la transformation numérique des secteurs d'activités, à participer activement à l'élaboration du cadre réglementaire et à son suivi, tout en fournissant aux services de l'État les moyens de faire face aux menaces.

EXPERTISE & recherche

Pour l'ANSSI, la recherche est une nécessité absolue, surtout si l'on considère la rapidité avec laquelle l'environnement technologique et les usages du numérique évoluent. Si l'objectif premier est celui d'un maintien à l'état de l'art, il est également important d'entretenir les capacités d'anticipation de l'agence et d'intégrer les spécificités des avancées techniques et des nouveaux protocoles comme des nouvelles plates-formes.

DES LABORATOIRES À L'EXPERTISE RECONNUE

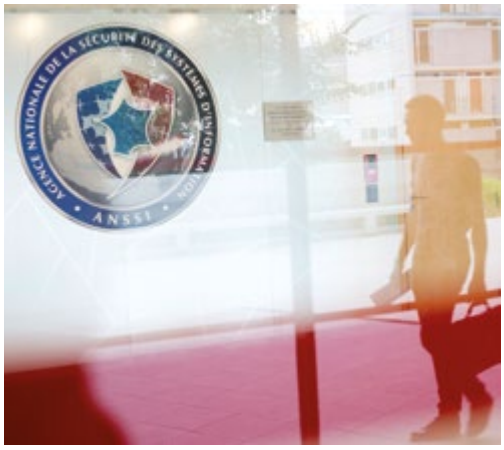
Six laboratoires, intégrés à la sous-direction Expertise, concentrent l'essentiel des activités de recherche de l'agence. Leurs domaines de compétence se répartissent entre la cryptographie, la sécurité des composants, la sécurité des technologies sans fil, les architectures matérielles et logicielles, les réseaux et protocoles, et les techniques de détection d'attaques. Ces structures aux rôles multiples sont à l'origine des référentiels techniques utilisés par l'ANSSI, et constituent donc un rouage essentiel des mécanismes d'évaluation, de labellisation et d'audit mis en œuvre par l'agence. L'élaboration de ces référentiels techniques est éclairée par le contact avec des infrastructures opérationnelles. Par exemple, en 2015, le laboratoire sécurité des technologies sans fil (LSF), en collaboration avec les équipes du Centre opérationnel de la sécurité des systèmes d'information (COSSI), a participé aux audits de sécurité d'infrastructures dépendant des opérateurs de téléphonie mobile. Ces laboratoires peuvent également contribuer à la création de produits sécurisés, à l'instar du laboratoire architectures matérielles et logicielles (LAM), qui consacre une part importante de son activité au développement du système d'exploitation sécurisé CLIP, dérivé de Linux et offrant une très haute résistance aux logiciels malveillants. Ces travaux donnent lieu à des contacts suivis avec des acteurs industriels, tels Airbus ou Thales, mais aussi avec des utilisateurs, administrations ou opérateurs d'importance vitale (OIV). Ils contribuent ainsi à la mission d'intermédiation de l'agence en matière de cybersécurité, qui passe à la fois par un encouragement à la production de solutions de sécurité et par leur promotion auprès des opérateurs.

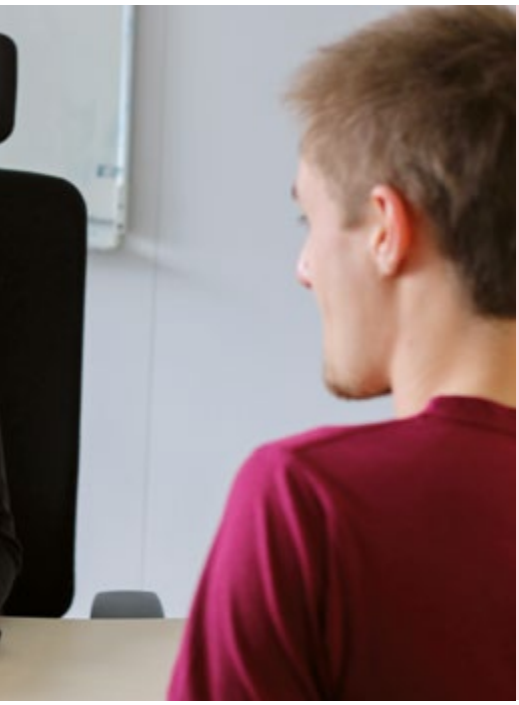
L'ANSSI veille à appuyer ses recherches sur les avancées enregistrées par le monde scientifique académique. À cet égard, la création en 2015 du laboratoire exploration et recherche en détection (LED) est représentative de la stratégie de l'agence en la matière. Ce laboratoire, dont l'activité est dédiée à la problématique de la détection d'attaques, mène des travaux de recherche en collaboration avec l'École normale supérieure (ENS) et l'Inria, comme avec les équipes internes de l'agence. Il assure ainsi un rôle de passerelle entre les savoir-faire de l'ANSSI et les outils et procédures utilisés par la recherche académique. Les transferts de compétence ainsi générés ont vocation à favoriser l'émergence d'applications concrètes en matière de cybersécurité. Dans la même optique, l'ANSSI accueille des doctorants en son sein (cinq en 2015) et encourage la validation par ses agents de leur expertise sous la forme de doctorats.

UNE LÉGITIMITÉ ET DES PARTENARIATS

Preuve de la légitimité et du dynamisme de la recherche dont fait preuve l'ANSSI, les travaux menés en son sein font régulièrement l'objet de publications à l'occasion de conférences scientifiques nationales et internationales. Ainsi, en 2015, pas moins de 40 publications ont vu le jour, sur des sujets aussi variés que la cryptographie, les interfaces de commande vocale de smartphones ou même les consoles de jeu. S'ajoute à ces publications le rapport de l'Observatoire de la résilience de l'Internet français, que l'ANSSI publie chaque année aux côtés de l'Association française pour le nommage Internet en coopération (AFNIC) et dont le but est d'identifier les interactions et dépendances entre les différents acteurs assurant le fonctionnement d'Internet en France. Ce rapport décrit également les axes d'amélioration et bonnes pratiques permettant d'assurer une résilience optimale de cette composante essentielle de la politique numérique française.

Les compétences portées par les laboratoires de l'ANSSI lui permettent de s'affirmer comme un acteur crédible au niveau international. Le laboratoire de cryptographie (LCR) collabore ainsi avec l'Office fédéral de la sécurité des technologies de l'information (BSI, Allemagne) sur des reconnaissances mutuelles d'évaluation, tandis que le LAM participe au suivi des travaux du groupe international Trusted Computing Group.





ANAËL, CHERCHEUSE AU LABORATOIRE EXPLORATION ET RECHERCHE EN DÉTECTION (LED)

« En 2014, à mon arrivée à l'ANSSI comme doctorante en application de méthodes d'apprentissage statistique appliquées à des problèmes de sécurité informatique, je ne peux pas dire que le domaine de la cybersécurité était ma spécialité.

Si je connaissais, bien entendu, l'agence de réputation, il s'agissait surtout pour moi de poursuivre mes travaux de recherche en m'appuyant sur des ensembles de données réels, par opposition aux ensembles simulés souvent utilisés dans les milieux purement académiques. C'est petit à petit, et surtout depuis la création du LED, que j'ai pu mesurer l'intérêt de travailler dans cet environnement si particulier.

Évoluer au sein de l'ANSSI m'a permis non seulement d'avoir accès à des données réelles, mais surtout de côtoyer des spécialistes reconnus en matière de sécurité informatique. Tout cela dans le cadre de projets dont les applications étaient des plus concrètes. En somme, je trouve ici le meilleur de deux univers. La collaboration du LED avec des structures comme l'École normale supérieure et l'Inria assure à nos recherches un contact permanent avec le haut niveau académique, tout en les confrontant aux évolutions et aux besoins concrets des acteurs de l'univers de la sécurité des systèmes d'information. En ce sens, ma mission s'inscrit dans le long terme, avec la perspective de pérenniser ce pont nécessaire entre deux mondes qui ont beaucoup à apprendre l'un de l'autre. »

FORGER LE CADRE réglementaire

Le domaine de la sécurité des systèmes d'information évolue au gré de l'apparition de nouvelles technologies, de nouveaux usages et donc d'angles d'attaque qui s'adaptent à ces bouleversements. Le cadre réglementaire doit pouvoir suivre et anticiper ces changements, en offrant aux différents acteurs, publics comme privés, un environnement sécurisé. En tant qu'autorité nationale en la matière, l'ANSSI joue plusieurs rôles dans ce processus. Elle conseille et appuie l'action des pouvoirs publics, et représente la France à l'échelon international, et en particulier européen.

UN TOURNANT LÉGISLATIF

Le cadre réglementaire dans lequel s'inscrit la mission de l'ANSSI a été modifié en 2015 par la parution de trois décrets d'application de la loi de programmation militaire (LPM) 2014-2019, relatifs à la sécurité des systèmes d'information. Ils concernent notamment les obligations des opérateurs d'importance vitale (OIV) et la qualification des prestataires de service, ainsi que la possibilité pour l'agence de requérir des opérateurs télécom l'identification des victimes d'attaques. Ces publications marquent une étape importante d'un processus législatif auquel l'ANSSI a pleinement participé, assumant son rôle d'autorité nationale en matière de sécurité des systèmes d'information.

Cette étape, aussi fondamentale soit-elle, ne signifie pas que le processus de traduction des objectifs fixés par la loi est achevé. Reste maintenant à élaborer les arrêtés sectoriels qui établiront les critères particuliers s'appliquant aux OIV. En effet, pour une efficacité optimale du nouveau dispositif, chacun de ces arrêtés devra prendre en compte les contraintes et les exigences propres à chaque acteur concerné.

À cette fin, l'ANSSI a lancé dès octobre 2014 des groupes de travail sectoriels réunissant les ministères concernés et les OIV des différents domaines dans le but de définir des règles de sécurité à la fois efficaces et adaptées à chacune des situations considérées. Cette période de transition entre acceptation des grands principes et équilibres de la loi et mise en œuvre effective s'avère délicate et essentielle, notamment pour identifier des problèmes encore non détectés. C'est seulement au terme de ce processus, au cours de l'année 2016, que seront publiés les arrêtés sectoriels.

YVES, COORDINATEUR SECTORIEL

« J'ai rejoint l'ANSSI pour servir l'État et découvrir d'autres champs d'application de la sécurité informatique. Ingénieur en génie des systèmes d'information et télécommunications, ayant réalisé une partie de mes études à l'École polytechnique de Montréal, j'ai en effet d'abord travaillé dans deux grandes banques, comme consultant au sein de l'équipe du responsable sécurité des systèmes d'information, puis comme responsable de la sécurité de l'information. L'activité interministérielle de l'agence m'a donc permis de découvrir d'autres domaines que celui de la finance. Comme tous les coordinateurs sectoriels de l'agence, je suis le point de contact privilégié des opérateurs de mon portefeuille (ministères, organismes privés de toutes taille…). Je priorise, oriente leurs sollicitations et assure un premier niveau de réponse à leurs questions en matière de sécurité informatique. Il s'agit essentiellement de prévention et de sensibilisation. Chaque année, je définis une stratégie pour les secteurs dont j'ai la charge, afin que leurs opérateurs atteignent une plus grande maturité en matière de sécurité informatique. Pour cela, je dois avoir une bonne connaissance des secteurs concernés, mais aussi des compétences des personnels de l'ANSSI, afin de pouvoir les mobiliser si nécessaire. Et, compte tenu du haut niveau du personnel de l'agence, il s'agit toujours de têtes bien faites, expertes dans leur domaine, ce qui est très agréable.»

L'INTERNATIONAL

Le cadre réglementaire de la sécurité des systèmes d'information ne peut se limiter aux seules frontières nationales. Depuis sa création, l'ANSSI participe aux négociations internationales relevant de son champ de compétence et représente la France dans de nombreuses instances multilatérales. En 2015, si cette actualité a été dominée par l'identification d'un accord politique au sein de l'Union européenne sur la directive NIS (voir page 36), l'agence a également assuré son double rôle de veille et de représentation au sein d'institutions dépendant de l'OTAN, de l'UE ou de l'ONU.
Elle conduit aussi le dialogue avec les autres agences nationales et se réjouit, à ce titre, du renforcement du partenariat avec l'Allemagne autour du développement d'une stratégie européenne pour la sécurité du numérique. Cette approche s'est traduite, entre autres, par la publication commune, avec le BSI, son homologue allemand, des spécifications préliminaires d'un « jeton » eIDAS en lien avec les travaux sur le cadre réglementaire de l'authentification et de la signature électronique.

LES BIENFAITS DE L'ANTICIPATION

L'Union européenne a initié dès 2013 un processus qui a débouché, en décembre 2015, sur l'identification d'un accord politique entre le Parlement européen et le Conseil de l'Union européenne sur la directive Network & Information Security (NIS). Les dispositions actées traduisent un succès de la vision française de la cybersécurité, avec la définition « d'opérateurs fournissant des services essentiels », notion voisine de celle des OIV, et l'obligation pour ces derniers de « prendre des mesures de sécurité appropriées et de notifier les incidents graves aux autorités nationales compétentes ». Cet alignement avec la philosophie de la LPM, à laquelle l'ANSSI a largement contribué au sein des institutions européennes, a pour conséquence deux textes très proches et complémentaires. La directive NIS permettra à l'ANSSI d'étendre son action auprès d'une palette d'acteurs plus large, comme les fournisseurs de services numériques. Parallèlement, pour les OIV qui auront mis en place les dispositions prévues par la LPM, l'application de la directive aura un impact limité.

DES SYSTÈMES D'INFORMATION sécurisés

Les différentes crises qui ont marqué l'année 2015 ont souligné le besoin pour les autorités nationales de disposer de moyens de communication fiables et totalement sécurisés. L'ANSSI, en partenariat étroit avec le Centre de transmission gouvernemental (CTG), apporte sa contribution en développant et en assurant le déploiement et le support technique de systèmes sécurisés de téléphonie fixe (Teorem), de visio-conférence (Horus) ou d'intranet (ISIS).

Pour élargir son offre et apporter la plus grande souplesse à l'utilisation de technologies sécurisées dans les systèmes d'information des ministères, l'agence poursuit par ailleurs son implication dans des projets utilisant une base matérielle commerciale et a fait l'acquisition d'une licence globale pour le logiciel de chiffrement de données de la société Prim'X.

DES RÉSEAUX ROBUSTES

Pour les pouvoirs publics, faire communiquer entre eux leurs représentants en toute sécurité et, surtout, en toute discrétion est une nécessité absolue. Dans ce but, l'ANSSI s'implique fortement dans le déploiement et le support des réseaux et terminaux utilisés pour les communications des autorités. Elle participe au renouvellement du parc des téléphones sécurisés Teorem en assurant le renouvellement des clés de chiffrement et la migration des terminaux vers la deuxième version du système, tout en testant et en se préparant au déploiement d'une troisième version prévue en 2016. Des actions similaires sont menées sur la solution de visioconférence sécurisée Horus, avec un effort particulier entrepris en matière d'amélioration de la qualité et de l'ergonomie. Les chantiers à venir concerneront en priorité le secteur de la téléphonie fixe sécurisée.

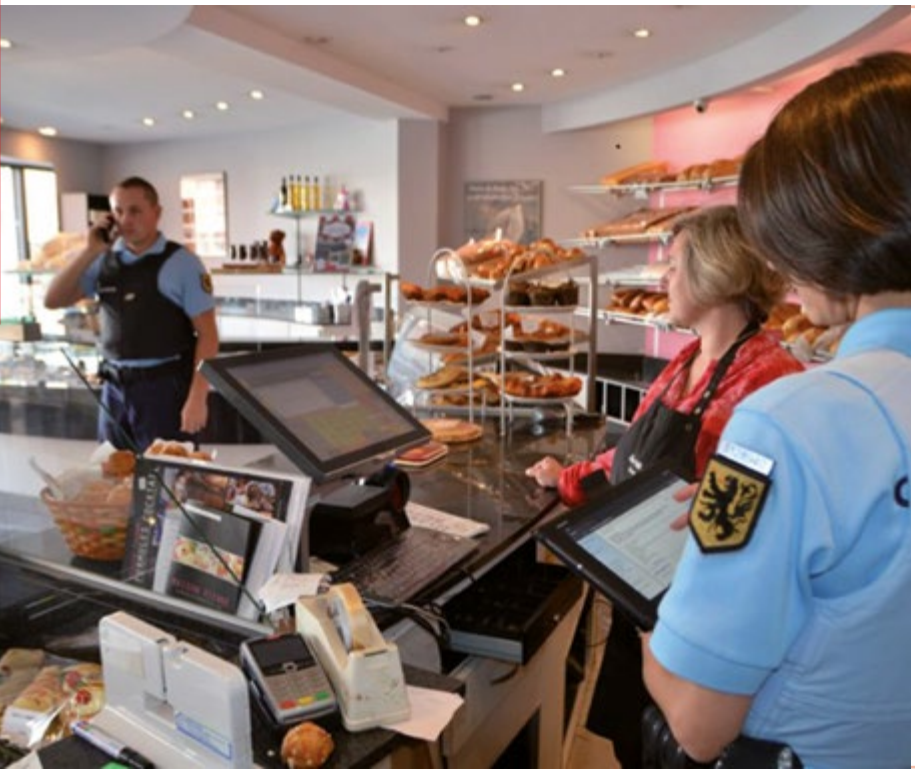
L'année 2015 a aussi vu la montée en puissance de l'intranet sécurisé interministériel pour la synergie gouvernementale (ISIS), homologué au niveau Confidentiel Défense. Parallèlement à l'élargissement de son emploi par les services de l'État, y compris hors situations de crise, ce système a remplacé la messagerie sécurisée MAGDA, qui équipait les préfectures. Cela s'est traduit par une densification importante du réseau, avec le déploiement de 500 terminaux supplémentaires, portant leur nombre total à 1 350. Pour mener à bien cette opération, l'ANSSI a œuvré aux côtés du CTG, qui a assuré le déploiement physique des postes.

JULIEN, CHEF DE PROJET SYSTÈMES SÉCURISÉS

« Après l'obtention de mon diplôme d'ingénieur et un master « Télécom et Réseaux », je me suis consacré, durant cinq ans, au développement de plates-formes pour les opérateurs téléphoniques dans le domaine de la voix sur IP.

Alors, en 2010, quand j'ai su que l'ANSSI cherchait un profil de ce type, j'y ai vu l'occasion de poursuivre dans cette voie, en intégrant la composante de sécurité. Si le sujet n'était pas spécifiquement lié à mes travaux, il m'intéressait, et quelle structure mieux que l'agence pouvait me permettre de creuser dans cette direction ?

À l'époque, déjà, la réputation de l'ANSSI, toute nouvelle structure créée à partir de la Direction centrale de la sécurité des systèmes d'information, en faisait une destination de choix. La motivation principale de ma candidature était d'ailleurs de pouvoir continuer à progresser au contact d'équipes compétentes, à la pointe sur leur sujet. De ce point de vue, je n'ai pas été déçu. Les tâches qui me sont proposées sont évolutives, en prise avec l'actualité technique et scientifique. Elles peuvent même revêtir un aspect grisant, au vu de l'ampleur que prennent nos sujets d'études. Travailler, comme je le fais avec mon équipe, au développement et au déploiement d'un système d'exploitation sécurisé pour smartphones (Secdroid) est une chose. Voir le résultat testé sur le terrain par 1 200 gendarmes dans le cadre de leurs missions quotidiennes donne une toute autre dimension à nos efforts. »



DES GENDARMES 3.0 !

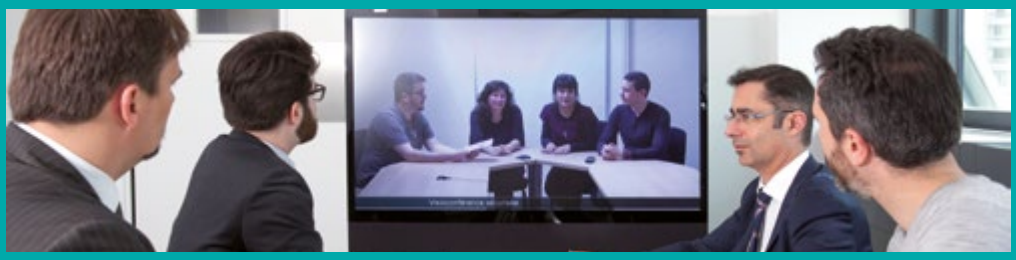
Comment offrir aux gendarmes plus de mobilité sur le terrain et un large accès aux applications métier spécifiques à l'exercice de leurs missions, le tout dans un environnement entièrement sécurisé ? C'est à ce besoin que la direction générale de la Gendarmerie nationale (DGGN) cherche à répondre à travers le projet NéOGEND, en dotant 1200 gendarmes du département du Nord de smartphones et de tablettes équipés du système d'exploitation Secdroid conçu par l'ANSSI. Cette expérimentation a donné lieu à une étroite collaboration entre les équipes de l'agence et celles de la DGGN, et à la mise en place d'une équipe de travail dédiée où sont représentées l'ANSSI et la gendarmerie. Pour les professionnels équipés, cette avancée permet d'envisager le développement de nombreuses autres applications métier (identification, procès-verbal numérique, interrogation de bases de données…), créant ainsi une nouvelle forme de proximité avec les citoyens en s'appuyant sur l'outil numérique.

SÉCURISER DE FAÇON INNOVANTE

En parallèle de ses efforts en développement de technologies propres, l'agence cherche également à explorer de nouvelles approches en matière de fourniture de solutions sécurisées aux pouvoirs publics. Cette philosophie a présidé au lancement de projets portant sur l'exploitation de smartphones et tablettes disponibles dans le commerce, dans le souci permanent de privilégier l'ergonomie. Ainsi, en 2015, Secdroid, un système sécurisé fondé sur l'architecture Android, a été porté sur le téléphone Samsung Galaxy S5+ et sur la tablette Sony XPeria 2. Une expérimentation à grande échelle de ce système est menée en collaboration avec la Police nationale et avec la Gendarmerie nationale qui a équipé, de façon expérimentale, 1 200 gendarmes dans le cadre du projet NéOGEND.

De la même manière, l'ANSSI s'est pour la première fois portée acquéreur d'une licence globale pour l'utilisation, par les services de l'État, d'un ensemble de logiciels de sécurité qualifiés auprès de la société Prim'X. Cette opération permet aux administrations de répondre à leurs besoins de sécurisation pour un coût de licence nul, ne laissant à leur charge que les frais de support. Cette initiative inédite permet à la fois d'optimiser la dépense publique et d'inciter les administrations à utiliser des produits de confiance tout en facilitant leur déploiement.

ACCOMPAGNER



L'ANSSI participe activement à la diffusion d'une culture de la sécurité du numérique et au développement d'un écosystème permettant la progression de la maturité nationale en ce domaine. À cette fin, elle mobilise de nombreuses ressources pour agir sur tout un ensemble de leviers, de la qualification à la formation, en passant par le soutien à l'innovation et au déploiement d'actions aux niveaux national et international.

GARANTIR LA QUALITÉ des produits

En matière de sécurité des systèmes d'information, la disponibilité de solutions sécurisées – produits, systèmes ou services – est fondamentale. Mais encore faut-il que la qualité soit au rendez-vous. L'ANSSI s'implique dans ce processus de mise à disposition de solutions de confiance, en labellisant des produits et des services de sécurité évalués selon des critères stricts, rassemblés dans des référentiels et appliqués par des centres d'évaluation indépendants agréés par l'ANSSI.

DES PRODUITS PASSÉS AU CRIBLE

Assumant le rôle d'autorité de certification nationale, l'ANSSI abrite le centre de certification national (CCN). Agréés par l'ANSSI, les centres d'évaluation de la sécurité des technologies de l'information (Cesti) sont indépendants et chargés d'évaluer la sécurité des produits ainsi que de vérifier leur conformité aux différents référentiels avant de délivrer certifications, qualifications ou agréments. Le CCN suit de près l'activité des différents Cesti. Tous les deux ans, le centre mène des audits pour s'assurer de leur compétence et de leur respect de bonnes pratiques. En 2015, pas moins de 88 produits ont été certifiés « critères communs » (CC) par l'agence, selon la norme ISO 15408, adoptée à l'échelle internationale par la plupart des pays industrialisés. Parallèlement, 8 produits ont obtenu une certification de sécurité de premier niveau (CSPN), de valeur strictement nationale, qui constitue une alternative plus rapide et moins coûteuse, et 150 certifications antérieures ont été renouvelées. Ces certifications correspondent à une évaluation neutre de la robustesse des fonctions de sécurité des produits, sans pour autant impliquer une recommandation d'usage par l'ANSSI.

Cette recommandation est, par contre, bien présente pour les produits qualifiés par l'agence. La démarche est cette fois plus longue, avec une évaluation en amont des capacités du produit, qui doit répondre à un besoin de sécurité avéré. Les produits qualifiés peuvent solliciter l'agrément de l'ANSSI pour attester de leur aptitude à protéger des informations classifiées ou à « Diffusion Restreinte ». Ils peuvent ensuite faire l'objet d'une seconde évaluation en vue d'un agrément OTAN ou UE. En 2015, 13 produits ont été qualifiés et 3 ont bénéficié d'un agrément.

DE LA QUALIFICATION À LA LICENCE GLOBALE

L'histoire des relations entre la société Prim'X et l'ANSSI reflète bien le potentiel de croissance que recèle une politique ambitieuse en matière de cybersécurité. Cet éditeur de logiciels lyonnais a fait le choix stratégique de faire passer tous ses produits par le processus de qualification de l'ANSSI, une décision forte qui n'allait pas sans un coût financier. Cette qualification et les certifications afférentes constituent une garantie, pour les clients de Prim'X, d'une qualité optimale des produits concernés. En 2015, la relation entre l'ANSSI et Prim'X, après des années de contacts étroits, a pris une autre dimension avec l'acquisition, par l'agence, d'une licence globale sur trois produits de sécurité proposés par l'éditeur, permettant ainsi aux services de l'État de s'équiper à leur convenance, en n'ayant à supporter que les frais liés au support. Pour la société, ce contrat inédit lui permet en retour de renforcer sa légitimité auprès des grands comptes et de l'international. Une démarche vertueuse et bénéfique pour tous les acteurs qui sera sans doute à renouveler pour d'autres types de produits.

UN PROCESSUS EN CONSTANTE ÉVOLUTION

Les démarches de certification, de qualification et d'agrément sont soumises à la pression constante des évolutions techniques, aux demandes des constructeurs, prestataires et utilisateurs, mais aussi à l'élargissement de leur périmètre d'application. Elles font l'objet de discussions permanentes aux niveaux national et international. Les ingénieurs du CCN participent ainsi régulièrement aux groupes de travail des instances de gestion des reconnaissances mutuelles, organisés dans le cadre du Common Criteria Recognition Agreement (CCRA) ou de l'accord européen de reconnaissance mutuelle (SOG-IS). Ils contribuent également à la promotion du schéma CSPN auprès de leurs partenaires européens.

L'ANSSI se penche en outre sur le problème posé par le succès même du processus de certification, qui se traduit par un afflux de demandes et une saturation progressive des capacités du CCN. Pour y faire face, une stratégie de réduction des délais de certification est en cours d'élaboration. Les procédures de qualification font, elles aussi, l'objet d'une réflexion de fond en vue d'en améliorer la lisibilité par les éditeurs de produits, de faciliter leur suivi dans le temps par les utilisateurs et d'introduire une gestion itérative des nouvelles menaces susceptibles d'affecter les produits qualifiés.

BENJAMIN, CHARGÉ DE QUALIFICATION DE PRESTATAIRES

« Mon arrivée à l'ANSSI ne doit rien au hasard. Depuis plus de dix ans, j'évolue dans le domaine de la sécurité de l'information. Après l'obtention d'un master en cybersécurité, j'ai été auditeur puis responsable adjoint du pôle technique d'un cabinet de conseil spécialisé en sécurité de l'information et, enfin, auditeur interne dans une grande compagnie d'assurance. C'est donc fort de ces diverses expériences que j'ai pris mes fonctions de chargé de qualification de prestataires à l'ANSSI, en 2015. Ce poste présente l'avantage de se trouver à la croisée des chemins de mes compétences et d'être en forte interaction avec de nombreux bureaux de l'agence. En fait, mon rôle est de remédier à un paradoxe : dans ses missions d'audit comme de détection et de réponse aux incidents, l'ANSSI est victime de son succès, ne peut répondre seule à l'ensemble des besoins et souhaite s'appuyer sur des acteurs privés. À ce titre, la qualification des prestataires de service en cybersécurité est une démarche essentielle, explicitement mise en avant dans la Stratégie nationale pour la sécurité du numérique édictée par le gouvernement. L'idée de contribuer aussi directement à un effort national est extrêmement valorisant, d'autant que les champs d'application à développer, du cloud aux systèmes industriels en passant par les technologies mobiles et l'Internet des objets, sont infinis. »

PROMOUVOIR LES SERVICES de confiance

La notion de prestataires de confiance a pris, depuis 2013, une ampleur inédite par la conjugaison de deux facteurs : la hausse constante de la demande émanant du secteur privé et l'effet accélérateur de la loi de programmation militaire 2014-2019 (LPM). Pour l'ANSSI, cette évolution s'est traduite par une augmentation significative des démarches de qualification de prestataires d'audit de la sécurité des systèmes d'information (PASSI).

RECHERCHE DE LA CONFIANCE

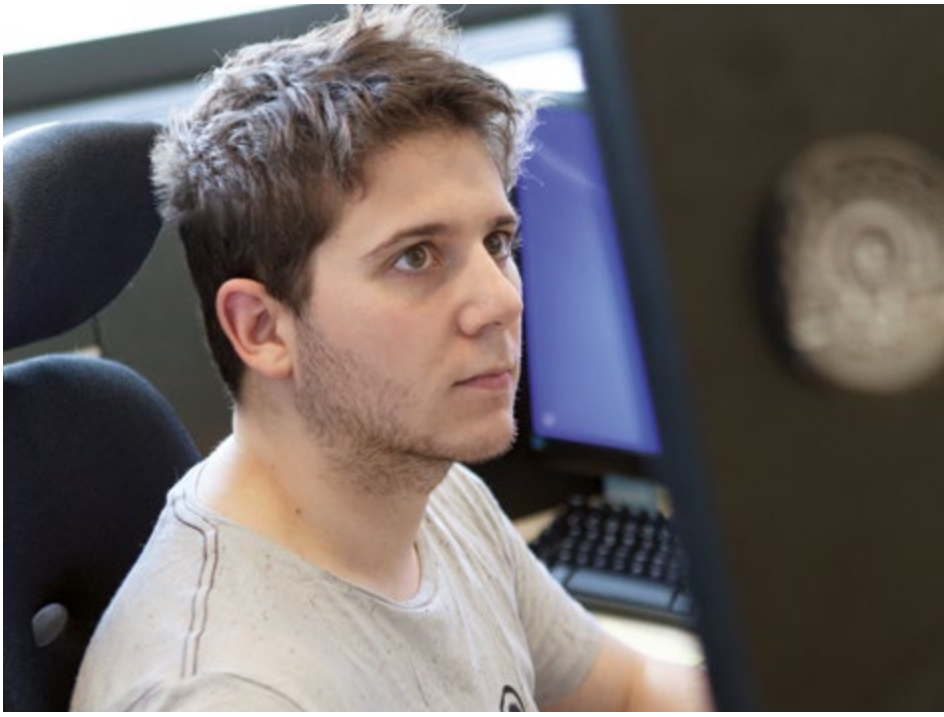
Même si l'agence poursuit sa mission d'audit auprès des services de l'État et des opérateurs d'importance vitale (OIV), elle ne peut suffire à couvrir tous les besoins, notamment en raison des nouvelles obligations en la matière que devront respecter les OIV dans le cadre de l'article 22 de la LPM.

En 2015, 9 PASSI ont ainsi été qualifiés, alors que 11 autres étaient en cours de qualification.

L'année a également été marquée par la nécessaire extension du processus de qualification à d'autres secteurs, tels que la détection des incidents de sécurité, la réponse aux incidents de sécurité et les services sécurisés d'informatique en nuage. Dans ces domaines, les référentiels sont en cours d'élaboration, grâce à la participation conjointe de centres d'évaluation et de futurs candidats à la qualification. Une fois la phase expérimentale achevée et les retours d'expérience intégrés, le processus de qualification entrera en fonction entre 2016 et 2017.

CONNAÎTRE ET PROMOUVOIR

Au-delà des seuls processus de certification et de qualification, l'ANSSI cherche continuellement à cartographier l'écosystème de la cybersécurité en France. En 2015, près de 350 rencontres bilatérales ont ainsi eu lieu entre l'agence et des entreprises de ce domaine. Cette connaissance approfondie et actualisée du secteur doit permettre d'identifier les acteurs et les besoins non satisfaits. Des rencontres multilatérales, comme le Forum international de la cybersécurité (Lille) ou les Assises de la sécurité et des systèmes d'information (Monaco), ont permis à la fois de rencontrer des sociétés proposant leurs produits ou leurs services, et de promouvoir auprès des acheteurs les solutions de confiance certifiées ou qualifiées par l'agence.



UN LABEL POUR ÊTRE RECONNU

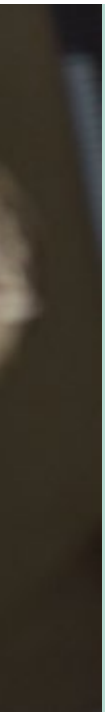
La création du label France Cybersecurity compte parmi les nombreuses actions de promotion de l'industrie française de cybersécurité. Cette distinction ne fait pas doublon avec les certifications et qualifications délivrées par l'ANSSI, même si ces dernières constituent un atout indéniable pour qui souhaite bénéficier du label. Il s'agit surtout de créer une identité qui permette de donner plus de visibilité aux acteurs de la filière de cybersécurité française, en particulier sur le plan international. Trois collèges assurent la gouvernance de la structure, représentant des groupements d'utilisateurs (Cigref, Gitsis, Cesin), des industriels (ACN, Hexatrust) et des représentants des structures étatiques (ANSSI, DGA, DGE). En 2015, 38 sociétés ont obtenu ce label.

Cette action de promotion s'est prolongée en direction des acheteurs publics, notamment par le biais d'une convention conclue avec l'Union des groupements d'achats publics (Ugap). L'objectif est de permettre la promotion des produits qualifiés par l'ANSSI dans les catalogues de l'Ugap ainsi que sa participation à la préparation des appels d'offres portant sur la cybersécurité.

CONTRIBUER AU DÉVELOPPEMENT

En 2013, le lancement par le président de la République de la Nouvelle France industrielle (NFI) avait été décliné en 34 plans, parmi lesquels le 33e plan, relatif à la cybersécurité. L'ANSSI avait été missionnée pour en assurer le pilotage. En 2015, lors du lancement de la seconde phase de la NFI, ce plan a rejoint une solution industrielle baptisée Confiance numérique, aux côtés des plans relatifs à la souveraineté des télécoms, aux logiciels et systèmes embarqués, à la nanoélectronique et au satellite à propulsion électrique. Sous cette nouvelle dénomination, l'ANSSI, qui assure la codirection de ce plan, poursuit les mêmes objectifs, à savoir notamment le développement des acteurs du secteur de la cybersécurité et leur promotion hors de nos frontières. En témoigne, par exemple, la création du label France Cybersecurity.

Le processus de certification et de qualification est, en lui-même, un outil de développement du secteur au plan national comme international. La prise en compte précoce de la cybersécurité en France et le rôle de l'ANSSI auprès des instances internationales en sa qualité d'autorité nationale en charge de la sécurité des systèmes d'information fait de la labellisation un argument de promotion des produits et des services qui l'obtiennent.



OLIVIER, ANALYSTE EN VULNÉRABILITÉS ET CODES MALVEILLANTS

« Après la détection d'une attaque, la réparation des dommages est évidemment nécessaire. Il ne faut pas pour autant négliger les éléments que peut apporter une analyse poussée des conditions de réalisation de l'intrusion. Depuis mon arrivée à l'ANSSI, en 2014, mon rôle est justement d'étudier les vulnérabilités qui ont été exploitées et les codes qui ont permis la réalisation de cette action. Le but ? Établir des indicateurs de compromission afin de prévenir ou de détecter les attaques. Pour ce faire, il faut en permanence remettre en question ses connaissances, et s'adapter à un domaine en perpétuelle évolution. C'est ce défi intellectuel qui m'a attiré, dès le stage qui concluait mon master de recherche en informatique. Je ne souhaitais pas forcément me consacrer à la direction de projet, comme la plupart de mes camarades de promotion l'ont fait, mais me mesurer à des défis plus concrets, plus pratiques. Travailler pour l'agence, dont la réputation n'est plus à faire en matière de sécurité des systèmes d'information, représentait un challenge passionnant et la promesse d'une émulation constante. Apprendre tous les jours, m'adapter, prendre en compte des enjeux nationaux, le tout au contact d'interlocuteurs aux profils variés, apportant des éclairages différents sur des thématiques techniques pointues, voilà la motivation qui m'était nécessaire. »

AUDIT, CONSEIL et assistance

L'ANSSI apporte également son expertise technique au Commissariat général à l'investissement (CGI), qui pilote les investissements liés au programme d'investissements d'avenir (PIA) et participe aux comités d'engagement du Fonds national pour la société numérique (FSN), créé dans le cadre du PIA. Elle s'est ainsi impliquée dans le dépouillement des réponses à l'appel à projets « Cœur de filière du numérique - sécurité numérique » et le suivi des projets retenus.

Les laboratoires de l'agence ont, par ailleurs, vocation à mettre leur expertise au service du développement opérationnel de solutions de sécurité par les industriels du secteur. En 2015, les travaux engagés autour du projet CLIP, système d'exploitation sécurisé sur une base Linux, se sont concrétisés par la mise en place de deux offres à destination des OIV, portées par Airbus et Thales. Depuis 2011, le code source de ce CLIP avait été mis à la disposition d'un certain nombre d'industriels, afin de favoriser l'émergence de produits de sécurité sur cette même base. Cette politique de prototypage et de reprise par des acteurs industriels a vocation à être étendue à d'autres domaines, tels que celui des architectures matérielles et logicielles sécurisées.

Enfin, l'ANSSI a renouvelé en 2015 son partenariat initié en 2005 avec Oséo, entreprise à capitaux publics qui finance les PME françaises dans une optique d'emploi et de croissance (elle-même intégrée depuis 2013 à la Banque publique d'investissement).

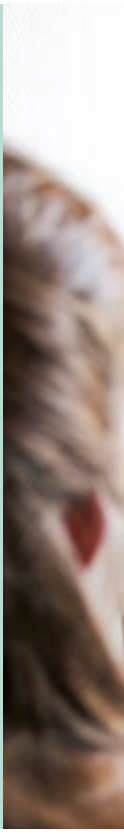
UN RÔLE DE CONSEIL

Pour appuyer le déploiement opérationnel des outils de sécurité par les administrations, l'ANSSI assume un rôle de conseil technique, qu'il s'agisse d'assister le service en charge du réseau interministériel de l'État, de participer à la préparation de la COP21 ou d'accompagner la Direction interministérielle du numérique et des systèmes d'information et de communication (Dinsic) dans le cadre du projet France Connect. Les OIV peuvent également solliciter l'agence,

VINCENT, CHARGÉ DE MISSION MAÎTRISE DES RISQUES ET HOMOLOGATION DE SYSTÈMES

« Le thème de la cybersécurité s'est invité progressivement tout au long de mon parcours professionnel, de mes débuts, au Centre national d'études spatiales (CNES), jusqu'aux années passées en bureau d'études. Aussi, lorsque j'ai décidé, en 2014, après quinze ans de carrière, de mettre mon expérience au service de l'État, l'ANSSI s'est imposée comme la structure adéquate. Travailler pour l'agence est donc une forme d'engagement, qui prolonge mon statut de réserviste opérationnel de l'Armée de l'air. Mais un autre élément essentiel pour moi était de continuer à apprendre, à évoluer. Sur ce point, je suis servi, et je ne m'attendais pas à ce que ce challenge soit quotidien !

Dans notre domaine, l'évolution de la menace est permanente, la réglementation s'adapte et de nouvelles solutions techniques apparaissent sans cesse. L'expérience ne suffit pas, la remise en question est continuelle. À mon poste, je me dois de comprendre les besoins des opérateurs et leurs demandes, puis d'orchestrer les réponses que peuvent apporter les ressources internes de l'ANSSI avec, comme fil d'Ariane, l'évaluation et la caractérisation du risque. Je suis également amené à représenter l'agence à l'extérieur, notamment dans le cadre des coopérations internationales, tout en assurant un rôle de formation et de conseil auprès d'opérateurs publics et privés. Toutes ces missions, au contact d'interlocuteurs très variés mais réunis dans leur culture du risque et leur exigence de sûreté, me confortent dans mon choix, sans doute au-delà de ce que j'escomptais.»



qui est à ce titre intervenue en 2015 auprès d'opérateurs tels ERDF, Areva ou Engie (ex-GDF Suez).
Des notes techniques sur des sujets généralistes comme l'administration sécurisée, la protection contre les dénis de service distribués ou la sécurisation des systèmes d'exploitation Linux et Windows sont régulièrement publiées, tandis que des fiches d'analyse particulières sont élaborées à destination des ministères et des OIV.
Enfin, l'agence mène des travaux de test des solutions utilisées par les différents opérateurs, qui servent à la rédaction de recommandations en matière de maîtrise des risques et d'homologation des systèmes.

LES SYSTÈMES INDUSTRIELS, NOUVELLES CIBLES

Pilotant et supervisant des installations industrielles de toutes tailles et de toutes natures, les systèmes de contrôle industriel sont de plus en plus souvent connectés à Internet. D'où une augmentation considérable de leur exposition aux cyberattaques. Cette vulnérabilité, accrue par le manque de maturité de ces installations en matière de sécurité des systèmes d'information, a été prise en compte par l'ANSSI dès 2012. C'est dans ce contexte que l'agence a piloté un groupe de travail dédié à ces questions. L'instauration d'un cadre global de traitement de cette problématique a ainsi été jugée prioritaire, s'agissant notamment de la certification de produits et de la qualification de prestataires de confiance pour les systèmes industriels. En 2015, une méthodologie de certification de produits de sécurité adaptés a vu le jour, tandis que quatorze profils de protection (pour chaque grande famille d'équipements) étaient publiés.

VÉRIFIER SUR LE TERRAIN

L'ANSSI mène régulièrement des audits de sécurité des systèmes d'information des services de l'État, soumis à des inspections cycliques réglementaires. Ainsi, chaque ministère doit, par exemple, se soumettre à une inspection, en principe tous les 3 à 4 ans, portant à la fois sur la sécurité des systèmes informatiques considérés comme prioritaires et sur l'identification d'axes d'amélioration adaptés. Ces audits peuvent également être sollicités par les administrations, notamment lors de la mise en œuvre de grands projets de systèmes d'information.

On observe la même distinction chez les OIV, qui peuvent faire des demandes d'audit, mais sont aussi soumis à des obligations en la matière, en vertu des dispositions sur les secteurs d'activité d'importance vitale. Ce cadre réglementaire va se trouver renforcé par l'application de la loi de programmation militaire 2014-2019, dont les décrets d'application relatifs aux obligations des OIV en la matière sont parus en 2015 et dont les arrêtés sectoriels sont en cours d'élaboration, en collaboration étroite entre l'ANSSI et les OIV.
Enfin, des audits peuvent également être déclenchés dans le cadre d'opérations de cyberdéfense, à la suite de la détection d'une attaque ou d'une intrusion.

FORMER et informer

En tant que chef de file de la cybersécurité sur le territoire national, l'ANSSI mène une politique de communication ambitieuse dont son nouveau site Internet est la vitrine. Elle contribue ainsi activement à l'entretien et à l'approfondissement de la culture de la sécurité du numérique chez tous les acteurs concernés, des administrations aux OIV, en passant par les établissements d'enseignement supérieur et les PME.

Pour ces raisons, l'agence est présente à de nombreux événements de sensibilisation et de communication autour des enjeux de la sécurité du numérique, qu'il s'agisse de conférences, de salons, de séminaires ou de rencontres internationales. L'actualité de l'année 2015 a ainsi été marquée par la participation de l'agence au Forum international de la cybersécurité, à Lille, aux Assises de la sécurité et des systèmes d'information, à Monaco, ou à la conférence C&ESAR, à Rennes, ainsi qu'aux événements organisés par l'Institut national des hautes études de la sécurité et de la justice (INHESJ) ou l'Institut des hautes études de défense nationale (IHEDN).

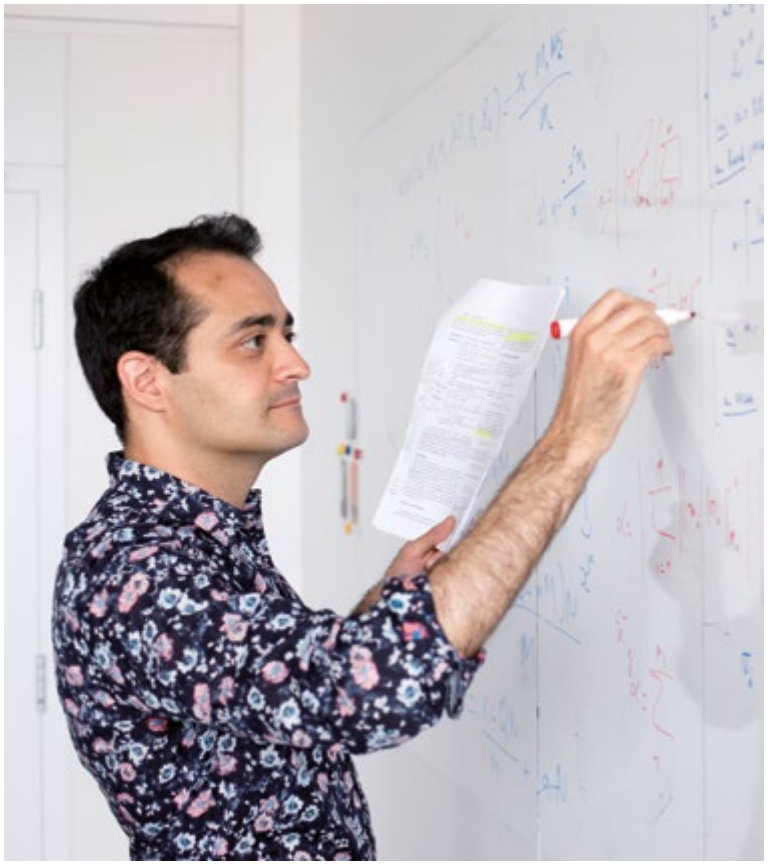
L'ANSSI a aussi organisé, le 16 octobre 2015, la présentation par le Premier ministre de la Stratégie nationale pour la sécurité du numérique. Enfin, elle s'est tenue à la disposition des médias lors des multiples crises qui ont marqué l'année (attentats de janvier et de novembre, cyberattaque de TV5 Monde...), en répondant aux sollicitations de la presse nationale et internationale et en communiquant aux journalistes les éléments nécessaires à la couverture de ces événements.

Mais la communication de l'agence est aussi dirigée vers des publics moins au fait des enjeux de la sécurité des systèmes d'information. En témoigne la campagne #Cybervigilant, venue rappeler les bonnes pratiques de sécurité et diffuser des messages encourageant la mise en place de précautions simples et élémentaires pour se prémunir des risques les plus répandus sur Internet.

De la même façon, l'ANSSI s'est associée à la Confédération générale des petites et moyennes entreprises (CGPME) pour éditer et diffuser un *Guide des bonnes pratiques de l'informatique*. Destiné à sensibiliser des structures qui, par faute de moyens, négligent souvent les cyber-risques, il rassemble 12 règles essentielles à la sécurisation de leurs équipements numériques.

FORMER, UNE MISSION ESSENTIELLE

Au sein de l'ANSSI, le Centre de formation à la sécurité des systèmes d'information (CFSSI) occupe une place centrale. Il remplit tout d'abord l'une des tâches stratégiques de l'agence, à savoir la formation des agents de l'État en matière de cybersécurité. À ce titre, il propose un important catalogue de stages



d'une durée d'une journée à cinq semaines, adaptés à la multiplicité des besoins et des profils. En 2015, 1 450 stagiaires ont participé aux 28 formations organisées par l'agence. Elles permettent la sensibilisation à différents aspects de la sécurité du numérique ou bien l'acquisition d'une expertise sur des sujets très variés, allant de la cryptographie à la sécurité électromagnétique en passant par la sécurité des réseaux sans fil.

Par ailleurs, le CFSSI assure une formation longue : celle d'expert en sécurité des systèmes d'information (ESSI). Étalée sur une durée de treize mois et sanctionnée par un titre de niveau I (bac +5), elle est inscrite au Répertoire national des certifications professionnelles (RNCP). En 2015, le titre d'expert a été attribué à 8 élèves au sein du CFSSI et, dans le cadre d'un partenariat, à 11 élèves de la voie d'approfondissement Sécurité des systèmes et réseaux, en formation d'ingénieur à Télécom SudParis. Le titre peut également être obtenu par le biais d'une validation des acquis de l'expérience (VAE).

L'ANSSI, dont le centre de formation est réservé aux agents de l'État, a par ailleurs œuvré au développement de ses relations avec d'autres organismes en charge de la formation en sécurité des systèmes d'information. Le but de cette démarche est de favoriser l'émergence d'une offre nationale en la matière, à même de répondre aux besoins sans cesse croissants du secteur. La même philosophie a présidé à la mise en place de CyberEdu, un projet de production de modules de formation « clés en main » à destination des enseignants qui a, lui aussi, donné lieu à de nombreux échanges avec l'enseignement supérieur. Cette démarche sera complétée en 2016 par l'aboutissement des travaux de l'agence sur la création de plates-formes de formation en ligne et sur la mise en place d'un schéma de labellisation de formations.

OLIVIER, CHEF DU CENTRE DE FORMATION

« À l'ANSSI, on n'est pas formateur de prime abord, on le devient. Ou, plus précisément, tout le monde est un formateur en puissance. Lors de mon arrivée à l'agence, après un master de recherche en informatique, j'ai rejoint la sous-direction Expertise, au sein de laquelle j'ai travaillé pendant huit ans, successivement dans les laboratoires consacrés aux systèmes, puis aux réseaux. Mais, dès les premières années, je me suis impliqué dans la formation, en parallèle de mes travaux de recherche. Cela s'explique par le fonctionnement un peu particulier du Centre de formation en sécurité des systèmes informatiques (CFSSI). Ici, pas d'enseignants professionnels, mais un recours systématique aux spécialistes en interne, les plus à même de répondre aux besoins spécifiques du centre. J'ai donc été sollicité pour des interventions, puis, petit à petit, la volonté de transmettre et le goût du partage des connaissances m'ont poussé à développer cet aspect de ma mission et je suis donc devenu responsable d'un module de formation. Pour moi, la formation est d'ailleurs un prolongement naturel de la recherche, une façon d'affiner sa pensée, de la préciser en cherchant à l'expliquer. Le dernier pas a été franchi en 2015, quand j'ai pris la responsabilité du CFSSI. Désormais, je suis l'un de ceux qui sollicitent les experts de la maison pour qu'ils assurent des formations. Pour autant, je n'ai pas abandonné la recherche et vais soutenir ma thèse à l'automne 2016. Cette double casquette est essentielle pour assurer la qualité du dialogue entre le CFSSI et les différents services experts de l'agence, qui abritent tous nos futurs formateurs. »

AGIR

Pour assurer la défense des systèmes d'information, une action coordonnée et efficace est indispensable. Afin de répondre aux attaques, de défendre les intérêts de la France et de développer une culture de la sécurité du numérique en France, l'ANSSI met en place les conditions d'une bonne coopération avec ses partenaires nationaux et étrangers.

VEILLE, DÉTECTION ET RÉPONSE aux attaques

En complément de ses activités de protection et de prévention, l'ANSSI est chargée de la défense des systèmes d'information des services de l'État et des opérateurs d'importance vitale (OIV). Une mission cruciale, remplie par le Centre opérationnel de la sécurité des systèmes d'information (COSSI).

RÉAGIR RAPIDEMENT

L'ANSSI assure une prestation de détection des cyberattaques auprès des services ministériels. Dans ce cadre, elle déploie sur leur réseau des sondes dont elle assure la mise en œuvre et le maintien en conditions opérationnelles. Le COSSI est chargé de leur supervision. En 2015, plus d'une dizaine de déploiements ont permis d'améliorer cette activité. La prochaine étape est l'installation, sur le réseau interministériel de l'État (RIE), de sondes de nouvelle génération, capables de supporter de très hauts débits.

L'agence, via la permanence opérationnelle du COSSI, active 24 heures sur 24 et 7 jours sur 7, reçoit et effectue ensuite un premier traitement des signalements d'événements de sécurité numérique.

Elle suit également en permanence l'actualité mondiale en matière de cybersécurité et diffuse chaque jour une revue de presse auprès de ses agents et de certains membres des services de l'État et opérateurs d'importance vitale.

UNE FORTE CAPACITÉ D'ANALYSE ET D'ÉVALUATION

L'ANSSI assure la collecte et la qualification des vulnérabilités et des codes qui les exploitent. En 2015, ses équipes ont identifié plus de 2 300 codes malveillants. Elles ont également rédigé près d'une vingtaine de rapports d'analyse.

Elles ont, en outre, publié 568 avis sur des correctifs de sécurité et diffusé 15 alertes sur des vulnérabilités critiques.

L'agence est par ailleurs chargée de l'anticipation et de l'analyse des risques et des menaces. En cas d'incident majeur, ses équipes réalisent notamment des notes de synthèse à destination des autorités gouvernementales.

MICKAËL, VEILLEUR SUPERVISION

« À l'ANSSI, je suis confronté certainement à ce qui se fait de mieux dans le domaine de l'informatique. La veille d'actualité nous permet d'être toujours à la pointe, de connaître les nouveaux produits intéressants et les dernières failles et attaques. Un atout certain dans l'exercice de mon métier, puisque je suis chargé de déterminer si les alertes émises par les détecteurs placés sur les différents sites du gouvernement révèlent une attaque ou tentative d'attaque informatique. En cas de menace avérée, je passe la main aux analystes. Et si j'ai choisi l'ANSSI pour rejoindre le secteur de la sécurité des systèmes d'information, aux perspectives d'évolution intéressantes, j'apprécie particulièrement notre autonomie et la vision verticale que nous avons de notre activité. Nous sommes également force de proposition, dans un esprit d'échange et d'interaction. Une façon de travailler très différente du secteur privé, où j'ai effectué le début de ma carrière ! Après un BTS Informatique de gestion, je me suis en effet dirigé vers l'alternance. J'ai notamment obtenu un double master Qualité, sécurité et environnement et en Ingénierie de l'information, tout en travaillant dans une entreprise qui conçoit et développe des solutions pratiques pour améliorer les relations téléphoniques. Et, à la fin de mon alternance, avant de rejoindre l'ANSSI, j'ai été administrateur réseaux dans une société de services en ingénierie informatique (SS2I). »

RÉPONDRE AUX ATTAQUES

Le COSSI traite tous types d'événements de sécurité informatique, rapportés par les sondes de détection installées par l'ANSSI, des partenaires français ou étrangers ou encore les victimes. En cas de nécessité, les équipes du centre peuvent se rendre sur place.

En 2015, l'activité de réponse aux incidents a connu une importante croissance : 4 000 signalements ont été reçus, soit 50 % de plus qu'en 2014. Cette augmentation est notamment due au développement, par des prestataires privés, de services de détection des attaques au profit des entreprises. Ces services seront rendus obligatoires pour les OIV dès la mise en application de la loi de programmation militaire du 18 décembre 2013. Ce texte imposera en outre de signaler à l'ANSSI les attaques subies. Après investigation, un grand nombre de signalements se sont avérés être des incidents de sécurité et ont été traités par le COSSI. Ce travail a permis de constater l'émergence de nouvelles attaques, dont les « rançongiciels », des logiciels malveillants chiffrant les données d'un ordinateur victime qui sont alors prises en otage le temps de payer une rançon.

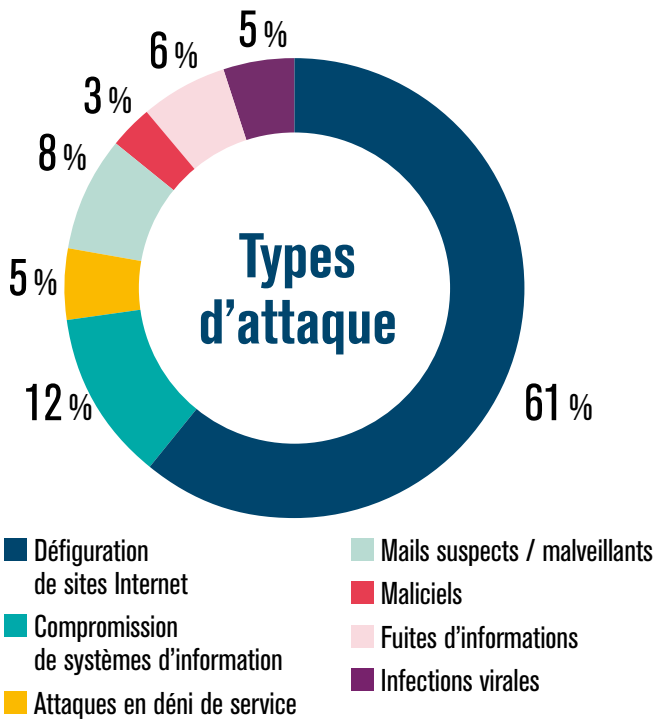
Le traitement des incidents repose également sur une bonne gestion des échanges entre l'ANSSI et ses partenaires, avec lesquels le COSSI entretient des relations opérationnelles. En 2015, l'ANSSI a développé les échanges (codes malveillants, rapports, signatures...) avec ses partenaires nationaux et étrangers, afin d'accroître ses capacités de détection des attaques.

En cas d'incident majeur et une fois sa gestion terminée, l'ANSSI procède à un retour d'expérience, afin d'en tirer des enseignements.

Au titre de la mission de prévention de l'ANSSI, le COSSI diffuse une partie de ces informations grâce à un bulletin d'actualité hebdomadaire publié sur le site Internet du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR). À partir des informations collectées lors de la gestion des attaques ou de travaux d'analyse de la menace, des campagnes d'information ou de recherche de compromissions sont menées auprès des services de l'État et des OIV. En 2015, plusieurs opérations de recherche de codes malveillants ont ainsi eu lieu.

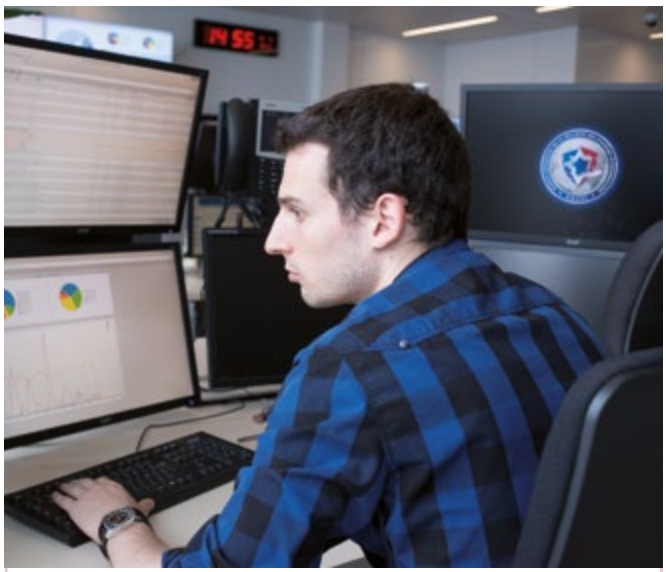
LA CONDUITE D'OPÉRATIONS D'ENVERGURE

En cas d'attaque de grande ampleur – comme le sabotage ou la prise de contrôle du système d'information à des fins d'espionnage –, une procédure spécifique de gestion est mise en place. En 2015, l'ANSSI a mené une vingtaine d'opérations de cet ordre. L'agence a non seulement travaillé à reprendre le contrôle des systèmes d'information victimes et à remettre en état les éléments compromis, mais aussi à renforcer leur sécurité. La plus emblématique de ces opérations est sans doute celle ayant suivi l'attaque des systèmes d'information de TV5 Monde (voir focus page 10).



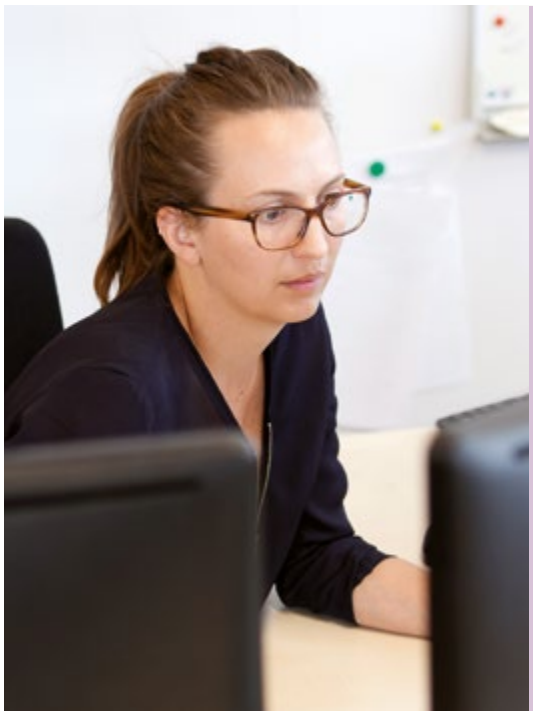
LA GESTION DE CRISE

En cas d'événement exceptionnel, l'ANSSI met en place un dispositif de crise, afin de coordonner les différents acteurs et d'apporter une réponse adaptée. Cette organisation permet également à l'agence d'être particulièrement flexible et réactive. En 2015, elle a été activée à quatre reprises : à la suite des attentats des 7, 8 et 9 janvier, du crash dans le sud de la France du vol 9525 de la compagnie GermanWings, le 24 mars, durant la période consécutive aux tragédies du 13 novembre en région parisienne et, enfin, à l'occasion de la la 21e Conférence sur le changement climatique « COP21 ». Lors de ces événements, l'ANSSI a été pleinement intégrée au dispositif interministériel de gestion des crises, quand ce dernier a été activé.



S'ADAPTER AU CHANGEMENT

Face à l'évolution de la menace, le COSSI anticipe la progression, en nombre comme en sophistication, des attaques informatiques. Il met également en place des processus opérationnels pour professionnaliser ses modes d'intervention, dans le cadre de la politique qualité de l'ANSSI. Il développe aussi son expertise technique (outillage, méthodes d'analyse…) pour se maintenir à l'état de l'art. Enfin, il améliore ses capacités de détection. L'année 2015 a notamment vu le développement des fonctions de veille, d'analyse et d'anticipation de la menace, sollicitées à la suite des attentats de janvier et de novembre en région parisienne, ainsi que lors de la COP21.



AUDE, INVESTIGATRICE NUMÉRIQUE

« Comment devient-on investigatrice numérique ? En cultivant une passion, celle de comprendre. Après avoir débuté ma carrière dans le secteur des télécoms, j'ai pu me rendre compte que les grands équipementiers et opérateurs français n'accordaient pas forcément aux enjeux de sécurité la même importance que les entreprises américaines, par exemple. Pourtant, j'avais envie de creuser le sujet et je ressentais le besoin d'en apprendre plus. J'ai donc profité d'un plan de départ volontaire pour réaliser une année de master, et c'est tout naturellement vers la sécurité des systèmes informatiques et des réseaux que je me suis dirigée. C'est d'ailleurs à cette occasion que j'ai eu mes premiers contacts directs avec l'ANSSI, par l'intermédiaire d'intervenants dans le cadre de la formation. J'avais la volonté de faire de la sécurité mon cœur de métier et la compétence des formateurs de l'agence m'avait convaincue : mon stage de fin d'année ne pouvait que se dérouler à l'ANSSI. Depuis mon arrivée, en 2014, mon activité consiste à repérer les traces qui me permettront de comprendre l'historique d'une cyber-attaque, son mode de propagation et l'état du système. Il y a en réalité un côté détective qui me plaît beaucoup dans ce métier. Et puis, travailler à l'ANSSI, c'est se trouver là où les choses se passent, à la pointe des questions de sécurité. Cela permet de toujours progresser.»

UN NÉCESSAIRE EFFORT collectif

Dans le domaine de la sécurité du numérique, la collaboration est indispensable. L'ANSSI entretient donc des liens étroits avec les ministères, les OIV, les acteurs locaux, afin de mettre en place des actions adaptées et coordonnées, mais aussi de mutualiser les ressources.

PRENDRE EN COMPTE LES BESOINS DES SECTEURS D'ACTIVITÉ

Depuis 2012, une équipe dédiée structure et coordonne les actions de l'ANSSI auprès des ministères et des secteurs d'activité d'importance vitale (SAIV). Son travail permet à l'agence de mieux appréhender les enjeux et les contraintes liés à chaque secteur d'activité et, ainsi, de mettre en place des actions adaptées. Elle veille également à la bonne intégration de l'ANSSI au sein des régulateurs et des acteurs étatiques de chaque secteur, ainsi qu'à l'articulation de ses initiatives avec les dispositifs existants.

En 2015, l'agence a ainsi travaillé sur les déclinaisons sectorielles des dispositions de la loi de programmation militaire (LPM) relatives à la cybersécurité, en concertation avec les ministères coordinateurs et les OIV. Elle a également apporté son appui aux ministères coordinateurs, dans le cadre de la révision des directives nationales de sécurité (DNS). S'ajoute à cela le soutien de l'ANSSI à des projets structurants au sein des SAIV et des administrations de l'État, comme le compteur Linky.

AU PLUS PRÈS DES TERRITOIRES

Plus récent, le dispositif d'action territoriale de l'ANSSI résulte de la volonté de toucher les acteurs locaux en relayant et coordonnant l'action de l'agence en région. Il contribue au partage d'expérience et à la mutualisation des rôles dans le domaine de la sécurité du numérique. Il est entré en phase opérationnelle en décembre 2015, avec la nomination des quatre premiers référents, affectés respectivement aux régions Île-de-France, Bretagne, Hauts-de-France et Auvergne-Rhône-Alpes. L'objectif est d'étendre ce dispositif à toutes les régions métropolitaines d'ici à décembre 2016.

AIDER LES VICTIMES DE CYBERMALVEILLANCE

En 2015, un groupe de travail interministériel, présidé par le ministère de l'Intérieur et l'ANSSI, a mis en évidence le besoin d'apporter des réponses concrètes à l'ensemble des victimes d'attaques informatiques, au-delà du périmètre actuel du COSSI (administration et OIV, principalement). Les modalités de création et de fonctionnement d'une plate-forme d'assistance dédiée, prévue par la Stratégie nationale pour la sécurité du numérique, devraient donc être définies en 2016. Cette plate-forme nationale accompagnera les victimes en les orientant vers des prestataires locaux et en facilitant les démarches administratives, dont le dépôt de plainte. Elle sera pilotée par le ministère de l'Intérieur et l'ANSSI, et fera notamment appel au réseau territorial de l'agence.

L'ANSSI À L'INTERNATIONAL

Tous les États sont confrontés à des problématiques de sécurité du numérique. La coopération à l'échelle internationale est donc une nécessité. Dans ce domaine, l'activité de l'ANSSI est pilotée par une équipe chargée de coordonner l'action de l'agence, de définir des axes stratégiques et de les défendre, et d'assister le directeur général dans son action à l'international. Toutes les sous-directions de l'ANSSI contribuent à cette mission, en témoignent les 202 réunions internationales auxquelles a participé l'agence en 2015.

DES RELATIONS DE CONFIANCE

L'ANSSI développe des relations bilatérales et multilatérales autour des questions de cybersécurité avec ses principaux partenaires de confiance, soit plus de trente pays parmi lesquels l'Allemagne, avec laquelle l'agence a renforcé et rendu public son partenariat autour du développement d'une industrie européenne de la sécurité numérique. Ces échanges, plus ou moins développés, sont de natures variées : dialogue stratégique, coopération opérationnelle... L'agence contribue par ailleurs à la mise en place d'une coordination interministérielle des activités d'assistance capacitaire. Elle soutient également des opérateurs dans la réponse à des appels d'offres internationaux relatifs au développement d'organisations nationales de cybersécurité. Elle participe enfin à l'ouverture du dialogue avec des pays qui hébergent des menaces importantes pour la France.

REPRÉSENTER LA FRANCE

L'ANSSI s'implique au sein de quatre instances internationales actives dans le domaine de la cybersécurité : l'Union européenne (UE), l'OTAN (Organisation du traité de l'Atlantique nord), l'ONU (Organisation des Nations unies) et l'OCDE (Organisation de coopération et de développement économique). Elle participe à l'élaboration des positions françaises et à leur défense, ainsi qu'à des groupes de travail. Elle prend également part à des exercices internationaux. Toutes ces activités sont menées en liaison étroite avec les administrations concernées. Grâce à un travail interministériel efficace, la France est l'un des pays les plus présents dans la majorité de ces organisations. L'ANSSI participe notamment à certains groupes du Conseil de l'Union européenne et au conseil d'administration de l'agence européenne chargée de la sécurité des systèmes d'information (ENISA). En 2015, la directive Network & Information Security (NIS) a fait l'objet d'un consensus politique (entre le Conseil et le Parlement), après trois ans de négociations auxquelles l'ANSSI a fortement contribué. Ce texte, qui reconnaît le rôle de l'Union européenne en matière de cybersécurité, élargit le périmètre d'action de l'agence. Sa transposition en droit français est prévue en 2016. L'ANSSI a, par ailleurs, pris part aux négociations sur les flux de données. Enfin, elle a suivi les travaux de la Commission européenne sur la création d'un marché unique numérique.

OLIVIER, RÉFÉRENT DE L'ANSSI POUR LA RÉGION HAUTS-DE-FRANCE (NORD-PAS-DE-CALAIS-PICARDIE)

« Je me suis engagé dans la Marine comme simple matelot en 1986, puis j'ai gravi les échelons jusqu'à devenir officier sous contrat. Je me suis progressivement spécialisé dans la sécurité des systèmes d'information, domaine dans lequel j'ai obtenu en 2005 un master de l'École pour l'informatique et les techniques avancées (EPITA). Ma carrière dans la Marine s'est conclue par un poste à l'OTAN. Mon contrat d'officier achevé, j'ai contacté l'ANSSI, qui m'a proposé un poste dans le domaine de la réglementation internationale. J'étais alors chargé de représenter l'agence auprès d'instances internationales lors des échanges sur la révision de documents de sécurité informatique. Mon poste actuel de référent ANSSI en région, créé en 2015, résulte de la volonté de l'agence de se faire entendre jusque dans les petites structures publiques (notamment les mairies) et privées (notamment les PME et PMI), au-delà de son cœur de cible, à savoir les ministères et les opérateurs d'importance vitale. En fait, j'agis presque comme un ambassadeur auprès d'acteurs locaux comme les chambres de commerce et d'industrie, les clubs de la sécurité de l'information régionaux (CLUSIR), les prestataires d'audit de la sécurité des systèmes d'information… Il s'agit notamment de développer et d'approfondir les échanges avec ces structures, d'être pour elles des « facilitateurs » et les animateurs de réseaux à faire grandir tout en leur garantissant assistance et conseil. Le tout dans une attitude proactive et non directive. C'est un travail intéressant, épanouissant et sans routine, puisque tout est à construire ! Les référents ont également la chance de bénéficier d'une vraie autonomie et de travailler au sein d'équipes très dynamiques. »

JEAN, CHARGÉ DE RELATIONS INTERNATIONALES

« J'ai intégré l'ANSSI comme stagiaire en 2014, à la fin de mes études. J'ai suivi le parcours franco-allemand de Sciences Po Lille, qui m'a permis d'obtenir, outre un master « Stratégie, intelligence et gestion des risques », un master de sciences politiques de l'université de Münster. Pendant mon stage à l'ANSSI, j'ai travaillé dans les domaines de la coopération entre États et du *capacity building*, c'est-à-dire de l'aide à la montée en compétence d'un pays. Ensuite, j'ai choisi de rester comme agent contractuel et j'ai été intégré au pôle coopération, qui gère les relations bilatérales. Il était important pour moi d'avoir un métier tourné vers l'international, dans la continuité de ma formation. Aujourd'hui, mon rôle est de faire en sorte que l'agence dispose de partenaires capables de relayer ses messages ou de lui fournir une expertise complémentaire. J'ai commencé par travailler sur différents sujets avec des pays qui entretiennent des relations assez souples avec l'ANSSI. En 2015, j'ai pris en charge la gestion d'un partenariat avec un État, dans tous les domaines de compétence de l'agence. Mon travail me met en relation avec l'ensemble des activités de l'agence. Il me permet ainsi de mieux appréhender les multiples composantes de la cybersécurité, un secteur en perpétuelle évolution. Ce métier est très stimulant, notamment grâce à un emploi du temps chaque jour renouvelé, et offre une réelle autonomie. À l'ANSSI, quels que soient l'âge ou l'expérience, on peut vraiment faire évoluer les choses. »

FAÇONNER LES FUTURES NORMES

L'ANSSI contribue à la normalisation dans le domaine de la cybersécurité. Pour cela, elle collabore avec l'ensemble des acteurs français concernés. L'agence apporte également son soutien aux industriels impliqués dans les instances européennes et internationales de normalisation. Elle participe, en outre, au renforcement de la coordination nationale dans ce domaine. En 2015, l'ANSSI a copiloté la révision des critères communs, un ensemble de normes ISO relatives à la sécurité des systèmes d'information. De plus, au sein de l'Afnor et du Comité européen de normalisation, elle a activement contribué aux travaux sur l'identification électronique et les services de confiance pour les transactions électroniques. Enfin, elle a participé aux activités de normalisation du Comité de la filière industrielle de sécurité (CoFIS).

DES MOYENS et des hommes

Faire face à la montée en puissance de l'ANSSI, veiller à sa bonne gestion… : les activités de soutien sont garantes du fonctionnement de l'agence. Elles comprennent notamment la gestion des ressources humaines, des systèmes d'information internes et du budget.

Du fait de sa montée en puissance, l'ANSSI connaît une importante croissance de ses effectifs, passant de 120 agents en 2009 à près de 460 à la fin de l'année 2015. L'équipe en charge des ressources humaines a donc pour mission de recruter des agents dans les délais, de limiter le *turn-over* et d'assurer la formation du personnel.

UNE POPULATION DE JEUNES CONTRACTUELS

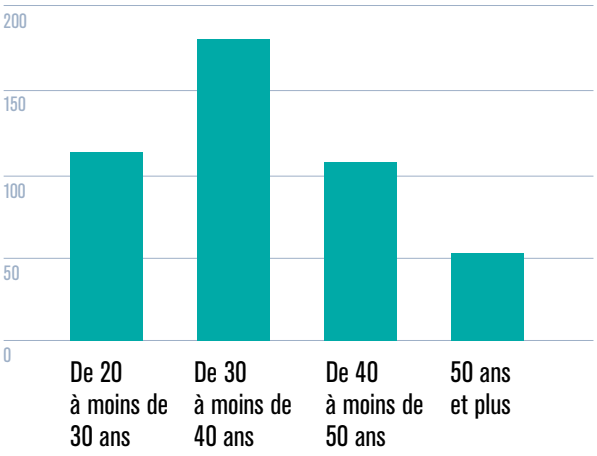
En 2015, 108 salariés ont rejoint l'ANSSI, dont 15 en fin d'études. Les deux tiers du personnel faisaient partie du Centre opérationnel de la sécurité des systèmes d'information (COSSI) et de la sous-direction Expertise (SDE). Du fait du domaine d'activité de l'agence, en constante évolution, 25 % des agents étaient âgés de moins de 30 ans, et 40 % avaient entre 30 et 40 ans. Enfin, trois quarts des agents étaient des contractuels, dont 73 % en CDD et 27 % en CDI. Le reste du personnel est composé de militaires (11 %) et de fonctionnaires (14 %). En effet, les profils recherchés par l'ANSSI sont rares dans la fonction publique.

DES POLITIQUES ACTIVES DE RECRUTEMENT ET DE FORMATION

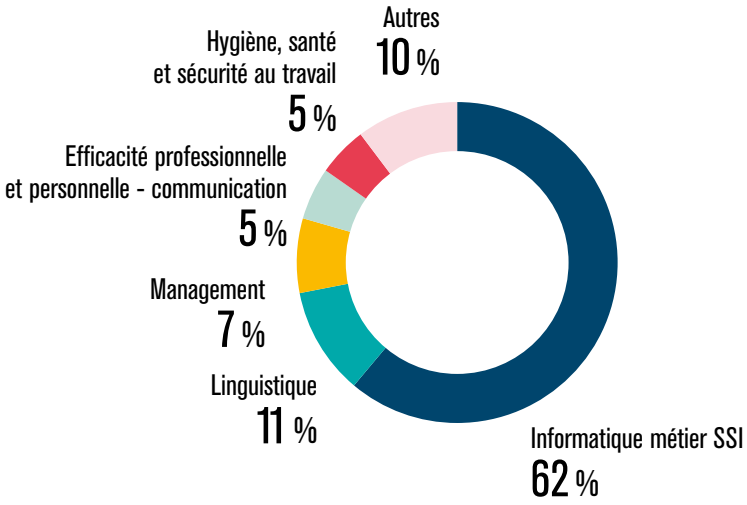
Pour attirer des candidats, l'ANSSI mène de multiples actions : diffusion des fiches de postes proposés auprès de 102 écoles, organisation de deux sessions de *job dating* à l'agence, participation à une dizaine d'événements, présence sur les réseaux sociaux professionnels…

Une fois recrutés, les agents se voient proposer de nombreuses formations. En 2015, cette politique a profité à près des deux tiers des personnels de l'ANSSI. Les sessions consacrées à « l'informatique métier SSI » ont représenté environ deux tiers des formations.

RÉPARTITION DE L'EFFECTIF PAR TRANCHE D'ÂGE À LA FIN DE L'ANNÉE 2015



RÉPARTITION DES FORMATIONS 2015 PAR CHAMP DE CONNAISSANCE



DES SYSTÈMES D'INFORMATION EN ÉVOLUTION

La croissance et l'extension des missions de l'ANSSI l'ont conduite à renforcer la fonction de gestion de son système d'information. Afin de créer une plus grande synergie entre les équipes informatiques de l'agence et le secrétariat général de la défense et de la sécurité nationale (SGDSN), les directions des systèmes d'information de ces deux institutions ont été regroupées le 1er juillet 2015. Cette réorganisation est entrée en vigueur au début de l'année 2016. Les équipes informatiques ont également accompagné la refonte du site Internet de l'agence. Enfin, 200 terminaux sécurisés (smartphones et tablettes) ont été attribués aux agents de l'ANSSI.

FINANCER LES PROJETS

En 2015, l'ANSSI a utilisé, pour ses projets, 28,53 millions d'euros en autorisations d'engagement et 36,95 millions en crédit de paiement. Elle a notamment travaillé à l'acquisition et à la maintenance d'équipements informatiques et de réseaux locaux pour son propre usage. Elle a également œuvré à la conception, à la réalisation, au déploiement, à la maintenance et à la gestion de dispositifs de communication électroniques sécurisés. Enfin, elle a acquis une licence globale permettant à l'administration d'adopter rapidement et massivement des produits recommandés et, ainsi, d'accroître son niveau de sécurité.

NATHALIE, CHARGÉE DE MISSION RH

« Je peux en témoigner : choisir l'ANSSI, c'est la garantie de travailler au sein d'une très belle maison, dans un esprit d'émulation intellectuelle et de partage des connaissances. Et, en plus, cela permet d'acquérir une jolie carte de visite ! Après une formation en allemand et un parcours de musicienne, j'ai commencé ma carrière à la Commission pour l'indemnisation des victimes de spoliation. En parallèle, j'ai suivi des cours du soir dans le domaine des ressources humaines au Conservatoire national des arts et métiers (Cnam). Quand j'ai postulé à l'ANSSI, en 2012, l'agence cherchait quelqu'un pour assurer le recrutement et gérer les liens avec les écoles. Ma mission consiste aujourd'hui à rechercher un maximum de profils pour suivre la montée en puissance de l'agence et aider les managers à construire leurs équipes. C'est un défi pour plusieurs raisons : un manque de notoriété de l'ANSSI qui pénalise le recrutement, un *turn-over* élevé au sein de l'agence qui s'explique notamment par la volonté de l'ANSSI d'essaimer les bonnes pratiques grâce à un flux renouvelé, sans oublier des compétences convoitées par les recruteurs d'autres secteurs. Nous menons donc un travail auprès des écoles et des universités pour attirer des profils juniors grâce à nos participations aux forums ou *job dating* et à nos collaborations avec des ambassadeurs issus de ces établissements. Nous envisageons également de diversifier nos événements de recrutement à destination, notamment, des profils seniors. »

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - communication@ssi.gouv.fr

www.ssi.gouv.fr
Twitter : @ANSSI_FR