2016

AGENCE
NATIONALE
DE LA SÉCURITÉ
DES SYSTÈMES
D'INFORMATION

Édité par l'Agence nationale
de la sécurité des systèmes d'information (ANSSI)
Directeur de la publication : Guillaume Poupard
Coordination : Séverine Oger
Conception et réalisation : Scripto Sensu
12, rue le chatelier – 75017 Paris, scriptosensu.com
Coordination éditoriale : Bertrand Vorimore et Lucie Toussaint
Crédits photos : Picturetank - Patrick Gaillardin
Picturetank - Florence Joubert / Picturetank - Patrice Normand
Bundesamt für Sicherheit in der Informationstechnik
Wikimedia Commons
Illustrations : Brian Wells Stevens

SOMMAIRE

L'ANSSI, ATOUT INDISPENSABLE À LA SOUVERAINETÉ DE L'ÉTAT

Louis GAUTIER,
secrétaire général de la défense
et de la sécurité nationale

Guillaume POUPARD,
directeur général de l'agence
nationale de la sécurité
des systèmes d'information

Le Secrétariat général de la défense et de la sécurité nationale (SGDSN) est chargé d'animer et de coordonner les politiques publiques concourant à la stratégie de sécurité nationale. À ce titre, le SGDSN est aussi un opérateur de sécurité dans certains domaines, dont la cyber sécurité. Il propose au Premier ministre et met en œuvre la politique gouvernementale en matière de sécurité des systèmes d'information. Il dispose à cette fin de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui lui est rattachée.

L'ANSSI est un atout majeur pour notre pays, alors même que les cyber menaces augmentent en nombre, en complexité et en nuisance. Tout en jouissant d'une très grande autonomie opérationnelle, elle bénéficie du positionnement interministériel et de l'accès direct aux autorités que lui confère sa place au sein du SGDSN. Ce rattachement de l'ANSSI au SGDSN est conforme à la place qu'occupe désormais la sécurité numérique dans les enjeux de souveraineté nationale. Il s'avère aussi très pertinent, car il permet au SGDSN d'intégrer les nécessités de la cyber défense dans les grands plans interministériels de réponse nationale aux crises qu'il conçoit. En matière de cyber défense, les autorités de l'État disposent ainsi d'une grande capacité de mobilisation et de réactivité, deux qualités indispensables dès lors que la menace numérique et le durcissement des systèmes de l'État et des opérateurs d'importance vitale, face à elle, s'inscrivent dans un schéma de long terme.

Au-delà des actions de prévention – en forte hausse – auprès des services de l'État, des opérateurs d'importance vitale, des entreprises, voire du grand public, l'ANSSI intervient aussi en cas de crise pour faire cesser les attaques et procéder à la réparation des systèmes informatiques agressés. L'ANSSI a montré en 2016 sa capacité à répondre à toutes sortes de sollicitations, dont certaines imprévues, comme, en 2015, lors de son intervention après le piratage de TV5 Monde. De façon générale, l'aggravation des menaces justifie de plus en plus souvent le recours à l'ANSSI, ce qui rend indispensable l'évolution de ses moyens financiers et humains au-delà de la programmation actuelle des effectifs d'ores et déjà réalisés, principalement constitués d'une ressource humaine d'une qualité exceptionnelle.

Louis GAUTIER

> **L'année écoulée a vu une progression très notable dans la prise de conscience du risque, et ce à tous les niveaux de la société.**

Le 7 juillet 2009, l'ANSSI voyait officiellement le jour sous la forme d'un « service à compétence nationale » essentiellement dédié à la sécurisation des systèmes d'information de l'État. Huit ans plus tard, il apparaît évident que l'univers dans lequel évolue notre agence a considérablement changé. Les attaques n'ont fait que s'accroître en nombre, en efficacité et en complexité. Sur ce plan, 2016 marque d'ailleurs une évolution significative, avec la concrétisation de nouvelles menaces visant à porter atteinte à la stabilité de nos démocraties.

Mais je veux aussi souligner que l'année écoulée a vu une progression très notable dans la prise de conscience du risque, et ce à tous les niveaux de la société. La sécurité numérique tend enfin à s'imposer comme un véritable enjeu de gouvernance dans les administrations et les entreprises tandis que nos concitoyens se montrent de plus en plus vigilants quant à la protection de leurs données personnelles.

Freiner la révolution digitale ? La question ne se pose pas : aujourd'hui, tout est numérique, et ce qui ne l'est pas le sera bientôt. Le vrai sujet est d'instaurer les conditions de sécurité indispensables à l'accompagnement de cette transition. Dans ce contexte, l'autorité nationale qu'est l'ANSSI renforce ses capacités d'action à tous les niveaux, qu'il s'agisse de confiance numérique, de protection de la souveraineté nationale, mais aussi de promotion des intérêts de la France à l'échelle internationale.

Pour ce faire, l'agence dispose d'atouts de poids : son statut interministériel au contact direct des plus hautes autorités via le SGDSN, ses missions uniquement concentrées sur la protection et la défense, et, bien sûr, ses capacités opérationnelles de très haut niveau. L'autre force de notre modèle tient au choix qu'a fait la France d'imposer la sécurité aux acteurs critiques, tout en veillant à maintenir en permanence un dialogue de qualité. Cela s'est concrétisé en 2016 avec la parution de la majorité des arrêtés sectoriels définissant les obligations des opérateurs d'importance vitale (OIV) en matière de sécurité des systèmes d'information.

Bien sûr, cette nouvelle donne réglementaire n'empêchera pas les attaques, mais nous avons collectivement enclenché une dynamique positive auprès des opérateurs concernés et avec l'ensemble des acteurs de la filière de la cyber sécurité. Avec la directive *Network and Information Security* (NIS) adoptée en juillet dernier, cette voie que nous avons suivie en pionniers est d'ailleurs amenée à devenir la règle en Europe à l'horizon 2018. C'est un signal positif pour la France et pour l'ANSSI, qui confirme une nouvelle fois sa capacité à coopérer à toutes les échelles et à fédérer un écosystème en faveur du développement de la confiance dans le cyber espace.

Guillaume POUPARD

EN UN COUP D'ŒIL

L'ANSSI EN SIX QUESTIONS

Service du Premier ministre, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Acteur majeur de la cyber sécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

1 QUEL RÔLE AUPRÈS DES HAUTES AUTORITÉS ET DES ADMINISTRATIONS ?

En collaboration avec les administrations compétentes, l'ANSSI instruit et prépare les décisions gouvernementales relatives à la sécurité du numérique et à celle des données sensibles. Elle participe également à la construction et à la maintenance des réseaux et des terminaux sécurisés pour les services de l'État. L'agence accompagne ainsi les cabinets du président de la République, du Premier ministre et des membres du Gouvernement dans la sécurisation de leurs systèmes d'information.

2 QUELLE MISSION AUPRÈS DES ORGANISMES D'IMPORTANCE VITALE ?

L'ANSSI accompagne les opérateurs d'importance vitale dans la sécurisation de leurs systèmes d'information critiques, rendue obligatoire par la Loi de programmation militaire de 2013. Cette sécurisation passe entre autres par l'application d'un corpus de 20 règles de sécurité définies par l'ANSSI et les opérateurs ainsi que la mise en place d'un dispositif de détection d'incidents et d'attaques.

3 QUELLE MISSION AUPRÈS DES ENTREPRISES ET DES CITOYENS ?

L'ANSSI est un acteur majeur de la promotion d'une culture de la cyber sécurité auprès des entreprises de toutes tailles et des particuliers, souvent moins au fait de ces problématiques. Ce positionnement se traduit par une politique ambitieuse de sensibilisation et d'accompagnement ainsi que par des actions relatives à la formation.

4 QUELLES RELATIONS AVEC LES AUTRES ACTEURS DE LA SÉCURITÉ NUMÉRIQUE ?

Parce qu'une agence ne peut pas, à elle seule, répondre à tous les besoins en matière de sécurité numérique, l'ANSSI se donne les moyens de favoriser un écosystème fiable. Pour ce faire, elle s'appuie sur ses propres savoir-faire, sur des coopérations avec des partenaires de confiance ou encore sur l'incubation de technologies et de dispositifs émergents. Elle contribue par ailleurs au développement de la recherche en matière de cyber sécurité afin d'anticiper les menaces et d'accompagner les évolutions technologiques.

5 QUELLE PLACE DANS LE CONTEXTE INTERNATIONAL ?

Le cyber espace amène à envisager la géopolitique et la géostratégie avec un regard neuf. À travers son engagement dans les négociations internationales et des stratégies de coopération bilatérale avec les États volontaires via des démarches de dialogue stratégique et un dispositif de soutien au développement capacitaire, l'ANSSI contribue activement au soutien des positions de la France dans le cyber espace. Son statut interministériel et son approche réglementaire font de l'agence française un modèle de référence qui intéresse un nombre croissant de pays alliés.

6 ET EN CAS D'ATTAQUE ?

En cas d'attaque avérée ou soupçonnée, le Centre opérationnel de la sécurité des systèmes d'information (COSSI) assure la défense des services de l'État et des opérateurs privés les plus sensibles. Pour mener à bien sa mission, le COSSI met en œuvre des dispositifs de veille, de détection, de collecte, d'analyse et de réponse aux incidents de sécurité.

EN CHIFFRES

UNE AGENCE ET 5 SOUS-DIRECTIONS

- Centre opérationnel de la sécurité des systèmes d'information (COSSI)
- Sous-direction Expertise (SDE)
- Sous-direction Systèmes d'information sécurités (SIS)
- Sous-direction Relations extérieures et Coordination (RELEC)
- Sous-direction Affaires générales (SDAG)

3 DIMENSIONS D'ACTION

Territoriale (plus de 500 interventions extérieures en 2016)
Nationale (hautes autorités + OIV : 300 entretiens bilatéraux en 2016)
Internationale (en relation avec plus de 40 pays en 2016)

CYBER DÉFENSE

20 opérations de cyber défense

3 235 signalements d'événements de sécurité numérique

Audits et contrôles

L'ANSSI a réalisé 59 audits auprès des ministères et des OIV

Audits à la demande : 60 %
Opérations : 28 %
Contrôles : 2 %
Inspections ministérielles : 10 %

PERSONNEL

500 agents

69 % du personnel de l'ANSSI a moins de 40 ans

27 % a moins de 30 ans

14 500 heures de formation en 2016, soit 29 heures de formation en moyenne par agent

25 % d'agents en sortie d'école

10 % de militaires

LABELLISATIONS

22 prestataires qualifiés (PASSI) et 17 en cours

95 certifications

16 produits qualifiés

PUBLICATIONS

Plus d'une vingtaine de supports de sensibilisation, dont le guide d'hygiène informatique recensant :

42 mesures de base pour une bonne hygiène informatique

45 publications scientifiques

INTERNATIONAL

80 missions pour défendre les positions de l'ANSSI à l'international

110 instructions pour la représentation française à Bruxelles dans le cadre de la construction de la directive NIS

L'ANSSI EN 2016

L'année 2016 restera placée sous le signe de la prise de conscience. Longtemps cantonné à une sphère d'experts, le sujet de la cyber sécurité est désormais perçu comme un enjeu fondamental par l'État, par les acteurs économiques, mais aussi par un nombre croissant de particuliers. Après avoir contribué à poser le débat, l'ANSSI est aujourd'hui en mesure d'actionner de nombreux leviers pour sécuriser la transition numérique en France et à l'international. Les événements qui ont rythmé l'année 2016 sont représentatifs de ce tournant majeur.

MARS

14-16 SecurityDays 2016 de Dakar. Organisé avec le soutien de l'ANSSI et de l'Agence de l'informatique de l'État sénégalaise, cet événement unique en Afrique de l'Ouest offre un cadre d'échanges entre experts militaires, civils, décideurs IT, chefs d'entreprise, industriels et utilisateurs finaux pour réfléchir conjointement aux problématiques liées à la cyber sécurité en Afrique.

JANVIER

25 et 26 Forum international de la cyber sécurité (FIC) de Lille. L'agence lance sa campagne de recrutement intitulée « Agir ensemble pour la sécurité du numérique ». L'objectif : passer de 500 à 600 agents au cours des deux années à venir.

FÉVRIER

4 Journée d'échange organisée en collaboration avec l'Union des groupements d'achat public (UGAP). Présentation et promotion des solutions et services de confiance labellisés par l'ANSSI. Ces derniers sont référencés sur le catalogue de la centrale d'achat publique au profit des administrations.

JUIN

9-12 Dans le cadre du dispositif général de sécurité mis en place au plan interministériel pour l'**« Euro 2016 »,** l'ANSSI a assuré plusieurs actions d'anticipation et d'appui auprès des organisateurs et des représentants du secteur audiovisuel au travers de recommandations et de conseils sur les questions de sécurité des systèmes d'information (SSI).

23 Publication des **premiers arrêtés sectoriels** pour les opérateurs d'importance vitale (OIV) des secteurs « produits de santé », « gestion de l'eau » et « alimentation ». Ces textes fixent les critères d'application des mesures relatives à la sécurité des systèmes d'information des OIV.

AOÛT

26 Publication des **arrê**
pour les OIV des secteurs
« gaz naturel », « hydroca
« transports terrestres », «
et fluvial » et « transport

MAI

11 L'ANSSI se dote d'une **stratégie ANSSI 2020.** Avec cette feuille de route évolutive, l'agence veut optimiser ses modes d'intervention afin de toujours mieux répondre aux nouveaux défis de la cyber sécurité.

26 Lancement officiel du **label SecNum*edu,*** programme de labellisation dédié aux formations supérieures en sécurité du numérique qui délivrent un grade de licence, licence pro, master, un titre d'ingénieur ou un master spécialisé.

JUILLET

1 Application du **Rè**
L'objectif : accroître l
électroniques au sein
en établissant un soc
électroniques sécuris
les entreprises et les

6 Adoption de la **dir**
Security (NIS), qui vi
harmonisées pour as
de sécurité des réseau
à l'échelle de l'Union

DÉCEMBRE

3-4 Publication des **arrêtés sectoriels** pour les OIV des secteurs « finances », « industrie », « communications électroniques et Internet », « audiovisuel et information ».

6-8 **Exercice PIRANET 16.** Rassemblant 170 personnes sur trois journées, cet exercice de niveau stratégique organisé par le SGDSN a permis de simuler une attaque de grande ampleur contre un ministère et un opérateur d'importance vitale du secteur de l'énergie.

13 Lancement du label franco-allemand **ESCloud** destiné à permettre à l'ensemble des acteurs européens de faire appel à des prestataires de services informatiques en nuage de confiance.

êtés sectoriels
s « énergie électrique »,
arbures pétroliers »,
« transports maritime
aérien ».

OCTOBRE

5-8 Participation aux **Assises de la sécurité et des systèmes d'information** à Monaco, un événement réunissant près de 2000 professionnels autour d'un programme de conférences, de *keynotes*, d'ateliers et de tables rondes.

7 Représentée par son directeur général Guillaume Poupard, l'ANSSI a été élue pour un an à la **vice-présidence du conseil d'administration d'ECSO** *(European Cybersecurity Organisation)*, qui fédère les acteurs du marché européen de la sécurité.

26 **Séminaire de sensibilisation** auprès des partis politiques. Organisé à l'initiative du SGDSN, ce rendez-vous a réuni les formations politiques représentées aux parlements français et européen pour faire le point sur les risques entourant l'élection présidentielle de 2017.

èglement européen eIDAS.
la confiance dans les transactions
n du marché intérieur
cle commun pour les interactions
sées entre les citoyens,
autorités publiques.

rective *Network and Information*
ise à établir des mesures
ssurer un niveau élevé et commun
ux et des systèmes d'information
européenne.

PANORAMA 2016
CYBER MENACE

Déstabilisation, sabotage de systèmes d'information, espionnage informatique, fraude, neutralisation et hacktivisme, les attaquants ont été plus que jamais actifs au cours de l'année 2016.

FRAUDE · DÉSTABILISATION · NEUTRALISATION · SABOTAGE · HACKTIVISME · ESPIONNAGE

ATTAQUES COORDONNÉES ET SIMULTANÉES À DES FINS DE DÉSTABILISATION

En novembre 2016, une campagne de déstabilisation a ciblé les États-Unis avant et pendant les élections présidentielles. Trois attaques ont notamment ciblé des organes et personnalités du parti démocrate.

VENTE D'ACCÈS SUR UNE PLATEFORME CYBER CRIMINELLE

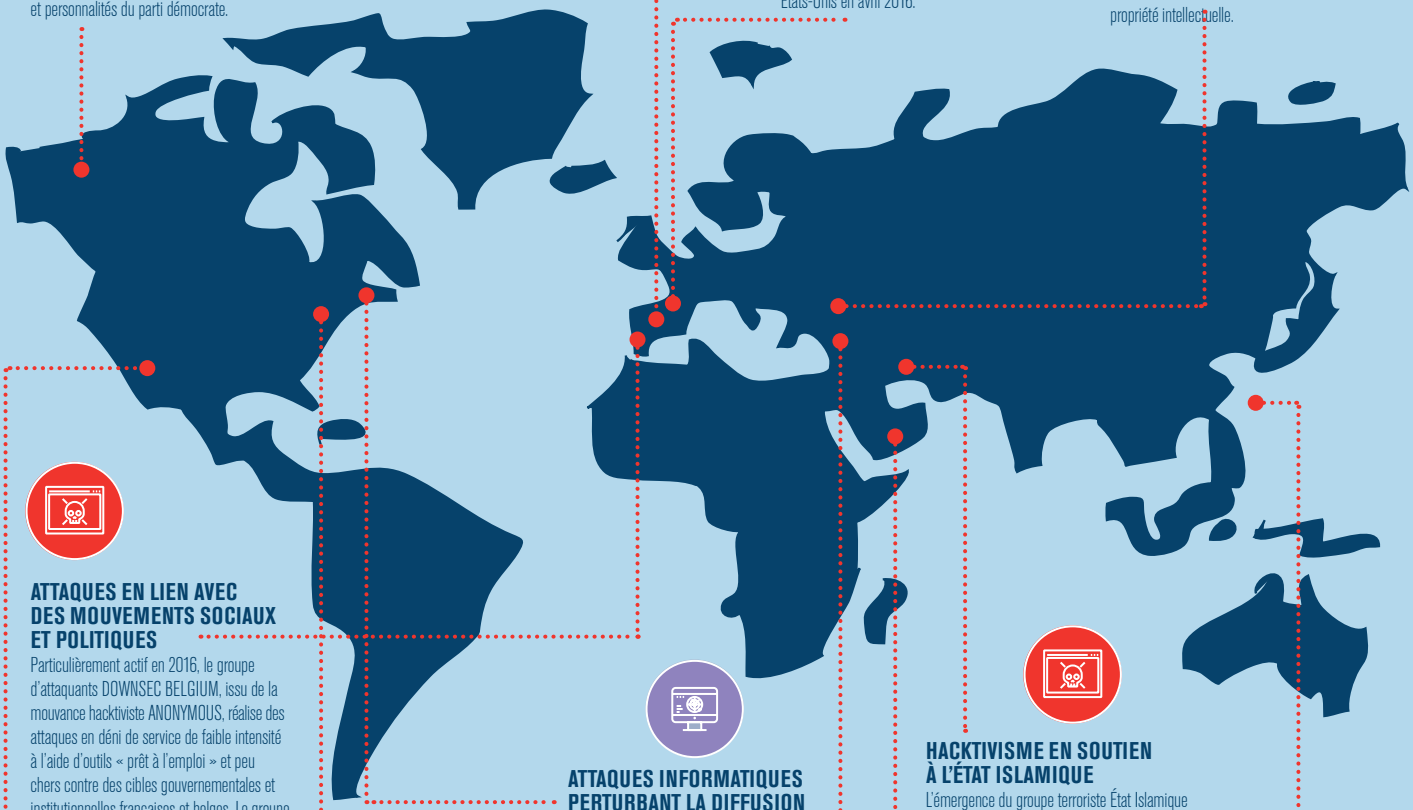
En juin 2016, une importante plateforme de vente cyber criminelle a été découverte. Elle proposait à la vente une liste de serveurs compromis, présentés comme appartenant à des réseaux privés ou gouvernementaux. Parmi ceux-ci, plus de 2 000 serveurs situés en France étaient listés.

RANÇONGICIEL : LOCKY

L'année 2016 a vu apparaître le rançongiciel LOCKY, doté de la capacité de chiffrer les fichiers accessibles via des partages réseaux, impactant ainsi l'ensemble du réseau auquel une machine infectée est connectée. LOCKY touche majoritairement la France. Il est aussi soupçonné d'être à l'origine de l'infection des systèmes d'information de dix hôpitaux aux États-Unis en avril 2016.

ESPIONNAGE INFORMATIQUE CIBLANT LE SECTEUR INDUSTRIEL

En juin 2016, la campagne d'attaques informatiques dénommée « Opération GHOUL » a ciblé principalement les secteurs de l'industrie et de l'ingénierie au Moyen-Orient. Les motivations des attaquants seraient financières, cherchant à exploiter des comptes bancaires et à revendre des éléments de propriété intellectuelle.



ATTAQUES EN LIEN AVEC DES MOUVEMENTS SOCIAUX ET POLITIQUES

Particulièrement actif en 2016, le groupe d'attaquants DOWNSEC BELGIUM, issu de la mouvance hacktiviste ANONYMOUS, réalise des attaques en déni de service de faible intensité à l'aide d'outils « prêt à l'emploi » et peu chers contre des cibles gouvernementales et institutionnelles françaises et belges. Le groupe est notamment en lien avec les manifestations contre la construction de l'aéroport de Notre-Dame-des-Landes et celles protestant contre l'adoption de la Loi dite « El Khomri ».

ATTAQUES INFORMATIQUES PERTURBANT LA DIFFUSION D'UNE CONFÉRENCE SUR LES MASSACRES DE TIANANMEN

Le 3 juin 2016, une vague d'attaques informatiques a ciblé le système d'information et le site Internet d'une association américaine, provoquant l'interruption de la diffusion en ligne d'une conférence sur le thème des manifestations de la place Tiananmen.

HACKTIVISME EN SOUTIEN À L'ÉTAT ISLAMIQUE

L'émergence du groupe terroriste État Islamique (EI) et l'évolution du conflit syrien ont été accompagnées par des campagnes de propagande diffusées sur les réseaux sociaux. Ces opérations ont pris la forme d'attaques informatiques telles que des défigurations de sites Internet et des divulgations de documents prétendument exfiltrés de systèmes d'information de gouvernements occidentaux.

EXFILTRATION MASSIVE DE DONNÉES CLIENT DE YAHOO

En septembre et en décembre 2016, l'entreprise américaine YAHOO a annoncé avoir été victime de plusieurs compromissions de son système d'information. Deux compromissions majeures ont abouti à l'exfiltration massive de données personnelles liées à près d'un milliard de comptes d'utilisateurs du service de messagerie.

ATTAQUES EN DÉNI DE SERVICE EXPLOITANT DES OBJETS CONNECTÉS

Au deuxième semestre 2016, des attaques en déni de service distribué (DDoS) d'ampleur inédite ont pu être réalisées grâce à des *botnets*[2] constitués de dizaines, voire de centaines de milliers d'objets connectés. Les attaques perpétrées contre l'un des principaux services d'hébergement américain de sites Internet, DYN, ont provoqué l'inaccessibilité de TWITTER, NETFLIX, AMAZON et OVH.

SABOTAGES INFORMATIQUES CIBLANT DES ORGANISATIONS ÉTATIQUES

Le 6 décembre 2016, jour de la fête de l'armée ukrainienne, le ministère des Finances et le Trésor ukrainiens ont été les victimes d'un sabotage informatique.

SABOTAGE INFORMATIQUE CIBLANT DES ORGANISATIONS

Le 17 novembre 2016, des entreprises et organisations étatiques saoudiennes, en particulier l'Autorité générale de l'aviation civile, ont été victimes de sabotage informatique.

ATTAQUES CIBLANT LES ENTITÉS CLIENTES DE SWIFT

Fin 2015 et début 2016, une campagne d'attaques informatiques a ciblé des entités bancaires clientes de la plateforme de messagerie interbancaire SWIFT[1]. Une trentaine d'ordres de paiement frauduleux auraient ainsi été émis par les attaquants pour un montant total avoisinant un milliard de dollars.

1 *Society for Worldwide Interbank Financial Telecommunication*. **2** Un *botnet* est un réseau de ressources informatiques préalablement corrompues et contrôlées par un ou plusieurs attaquant(s), pouvant servir à différentes finalités : diffusion de codes malveillants, émission de pourriels en masse, puissance de calcul, attaque en déni de service, rebonds/*proxy* afin de dissimuler son activité, etc.

STRATÉGIE ANSSI 2020
UNE FEUILLE DE ROUTE EN SIX AXES

Déclinaison du *Livre blanc sur la défense et la sécurité nationale* de 2013 et de la Stratégie nationale pour la sécurité du numérique adoptée en 2015, la stratégie ANSSI 2020 présentée en mai 2016 a été conçue comme une feuille de route souple et évolutive. L'enjeu : permettre à l'ANSSI d'être, dans ses métiers, une agence de référence en Europe.

À l'heure où les cyber attaques se multiplient et où chaque nouvelle technologie se double de nouvelles menaces, le développement numérique ne peut plus se concevoir sans sécurité et sans une approche multilatérale et internationale du cyber espace. Dans ce contexte en perpétuelle mutation, la stratégie ANSSI 2020 décline de manière opérationnelle la Stratégie nationale pour la sécurité du numérique et fixe le cap et les champs d'intervention de l'agence.

1 Connaître et anticiper

Accentuer la capacité d'anticipation de l'évolution des technologies et des usages pour favoriser l'action en amont, concentrer les ressources sur les meilleurs leviers.

2 Influencer et piloter

Renforcer l'ANSSI dans son rôle d'autorité nationale et de régulateur, accroître son domaine d'action et son impact.

3 Accompagner

Favoriser une connaissance fine et actualisée des publics de l'ANSSI afin d'adapter son action en fonction de leurs besoins et de leur niveau de maturité, élargir et renforcer l'offre de remédiation pour améliorer la résilience de la société française face aux attaques informatiques.

4 Défendre

Améliorer la connaissance et l'anticipation de la menace, accroître la réactivité de l'agence, la doter des capacités nécessaires pour faire face à une crise informatique majeure.

5 Coopérer, promouvoir

Favoriser le rayonnement international de la vision française de la cyber sécurité et de la défense, soutenir la politique étrangère de la France et le développement des entreprises françaises actives dans le domaine du cyber.

6 Soutenir

Améliorer le fonctionnement général de l'agence par une meilleure gestion des fonctions support (ressources humaines, finance, logistique…), favoriser le bien-être au travail des agents et leur offrir une visibilité accrue sur leur parcours professionnel.

Une feuille de route évolutive

La stratégie ANSSI 2020 établit une feuille de route pour les trois années à venir. Ce référentiel d'orientations et de projets structurants apporte une visibilité à l'ensemble des agents et des administrations partenaires de l'ANSSI. Dans un espace numérique en mouvement permanent, cette stratégie évolutive par nature fera l'objet d'actualisations annuelles.

"Avec la stratégie ANSSI 2020, nous avons voulu donner un cap commun en allant au-delà de la simple transcription interne de la Stratégie nationale pour la sécurité du numérique. C'est une démarche de développement qui permettra de fédérer toutes les compétences de l'agence pour consolider ce qui a déjà été entrepris, améliorer nos modes de fonctionnement et préparer l'avenir."

Guillaume Poupard

Et maintenant ?

Depuis la publication interne d'ANSSI 2020, 43 actions ont été définies et sont en cours de réalisation. Un dispositif de suivi d'avancement du plan d'actions a par ailleurs été mis en place avec des rendez-vous mensuels et des revues semestrielles au niveau du comité de direction.

1. DÉVELOPPER LA CONFIANCE

45
publications scientifiques

500
interventions en région

140
événements en France et à l'étranger

NUMÉRIQUE

Les services de l'État, les entreprises et les individus sont de plus en plus connectés par des technologies offrant de nouveaux modes de travail, d'interaction et de transaction. Sous la pression de la mobilité, de l'utilisation massive des données ou encore de l'Internet des objets, le numérique se diffuse toujours plus rapidement et profondément, plaçant la confiance numérique au rang des grands enjeux politiques, économiques et sociétaux. Par son rôle dans la définition du cadre réglementaire du numérique, ses actions de sensibilisation et ses stratégies de coopérations multiformes, l'ANSSI place la confiance numérique au cœur de ses missions.

CRÉER UN ENVIRONNEMENT FIABLE : RÉGLEMENTER ET ACCOMPAGNER

L'année 2016 marque un tournant par la prise de conscience des enjeux numériques en matière stratégique, économique, sociale et géopolitique. Agence interministérielle proche des plus hautes autorités, l'ANSSI bénéficie d'un positionnement lui permettant de favoriser l'instauration d'un environnement de confiance et de sécurité propice à la transition numérique. La concertation et l'implication de tous les acteurs, privés et publics, contribuent à faire de la cyber sécurité un sujet clé de gouvernance.

UN CADRE RÉGLEMENTAIRE ÉVOLUTIF AU SERVICE DE LA **TRANSITION NUMÉRIQUE**

Le domaine de la sécurité des systèmes d'information évolue au gré de l'apparition de nouvelles technologies, de nouveaux usages, de nouvelles menaces, et donc de nouvelles victimes. 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, l'ANSSI a pour mission de proposer au Premier ministre la politique nationale en matière de sécurité des systèmes d'information qui garantit la protection de la souveraineté nationale auprès des autorités et favorise la compétitivité de la France sur la scène économique. Pour ce faire, l'ANSSI participe notamment à la régulation, à l'encadrement des bonnes pratiques de SSI, à l'élaboration de référentiels normatifs en matière de sécurité numérique, à l'intégration des normes juridiques et techniques dans les schémas nationaux ainsi qu'à la mise à jour des textes réglementaires. En outre, l'agence assiste les ministères dans l'élaboration et la mise en œuvre des textes nationaux et internationaux liés à la sécurité des systèmes d'information (accords, guides, recommandations…).

"Nous sommes à un moment de rupture numérique, c'est une révolution industrielle et sociétale. Tous les pans de la société sont transformés, indissociables de la sécurité du numérique. Chacun doit être conscient de sa responsabilité."

Notre Nation a fait le choix d'un modèle original en rattachant l'ANSSI au Premier ministre via le SGDSN, lui conférant d'emblée une stature interministérielle en proximité avec les plus hautes sphères de décision, mais aussi avec les acteurs qui œuvrent sur des champs d'activité plus larges, notamment les ministères régaliens. Une autre force de notre modèle est d'avoir compris très tôt que les "bons conseils" ne suffisaient pas au vu de l'importance de l'enjeu. ***En choisissant de faire de la cyber sécurité une obligation pour les opérateurs d'importance vitale, nous avons pris une décision courageuse.*** *Aujourd'hui, la voie réglementaire que nous avons suivie commence à faire école, comme en témoigne la récente directive européenne NIS* (voir pages 38-39). *Mais comment imposer une sécurisation si les principaux concernés n'ont ni les moyens ni les compétences nécessaires pour s'y conformer ? Pour permettre aux opérateurs d'importance vitale d'être au rendez-vous des exigences de la loi de programmation militaire, l'ANSSI s'investit aujourd'hui pleinement dans la construction d'un vaste écosystème transdisciplinaire entièrement tourné vers la cyber sécurité. C'est une nouvelle facette de notre mission qui vise plus que jamais à conjuguer confiance numérique et souveraineté nationale. »*

Guillaume Poupard, directeur général de l'ANSSI

En 2016, l'activité réglementaire de l'agence a notamment été marquée par :

➔ la publication des référentiels liés à eIDAS. Adopté en juillet 2014, ce règlement instaure un cadre européen en matière d'identification électronique et de services de confiance afin de faciliter l'émergence du marché unique numérique. L'ANSSI intervient à double titre dans l'application du règlement : en tant que garante de la sécurité pour le volet « identification électronique » et en tant qu'organe de contrôle pour le volet « services de confiance ». Cette seconde mission l'a amenée à construire des référentiels d'exigences applicables aux prestataires de services de confiance qualifiés ainsi qu'à prononcer les premières qualifications « eiDAS » de prestataires de services de confiance en France ;

➔ l'élaboration des mesures d'application de la Loi pour une République numérique, notamment sur l'identification électronique, le coffre-fort numérique et l'envoi recommandé électronique ;

➔ les travaux engagés dans le cadre de la refonte en profondeur de l'Instruction générale interministérielle n° 1300 de 2011 qui organise la protection du secret de la défense nationale ;

➔ la contribution à différents chantiers engagés autour de la cohérence et de la convergence des textes réglementaires relatifs à la sécurité numérique et aux moyens cryptographiques des institutions internationales – Otan, Union européenne… – ainsi que de leurs programmes (Galileo).

Un appui juridique

Les activités de l'ANSSI, toujours plus nombreuses, diverses et complexes, impliquent un soutien juridique permanent. Avec la création d'un bureau dédié en 2016, l'agence dispose désormais de l'assistance juridique générale nécessaire à l'exercice de ses missions, ce qui se traduit par l'identification des risques juridiques, la veille et la rédaction de projets de textes normatifs, de conventions et d'accords de partenariats.

DES RÉSEAUX SOUS PROTECTION

Fonctionnement de l'État, activité économique, vie quotidienne… Les réseaux de télécommunications sont aujourd'hui omniprésents. Ils sont aussi exposés à des menaces qui se renouvellent en permanence. Leur sécurisation est un enjeu clé pour l'ANSSI.

Préserver les libertés individuelles

L'agence joue un rôle central dans le contrôle réglementaire instauré en application de l'article 226-3 du Code Pénal qui soumet à autorisation la commercialisation et la détention d'équipements susceptibles de porter atteinte à la confidentialité des communications électroniques. Ce régime de contrôle a été étendu en 2016 par un arrêté pris conformément aux dispositions de la loi de programmation militaire de 2013 (LPM). Il couvre désormais les « stations de bases » qui assurent la desserte radio des réseaux de téléphonie mobile, dès lors que ces équipements intègrent des fonctionnalités susceptibles de permettre le détournement des communications. Ces nouvelles mesures, assorties d'un délai d'application de cinq ans, permettront d'anticiper les évolutions technologiques de ces réseaux, tout en préservant les propriétés de sécurité attendues.

Analyser l'Internet français

Créé en 2011 sous l'égide de l'ANSSI, l'observatoire de la résilience de l'Internet français contribue à améliorer la compréhension collective de ce réseau par l'étude des technologies susceptibles d'entraver son bon fonctionnement. Associant les acteurs de l'Internet, dont l'Association française pour le nommage Internet en coopération (Afnic) et les opérateurs, il s'attache à apporter notamment au travers de son rapport annuel une vision cohérente et complète de l'Internet français, à identifier des indicateurs représentatifs de la résilience du réseau et à définir les bonnes pratiques qui en découlent.

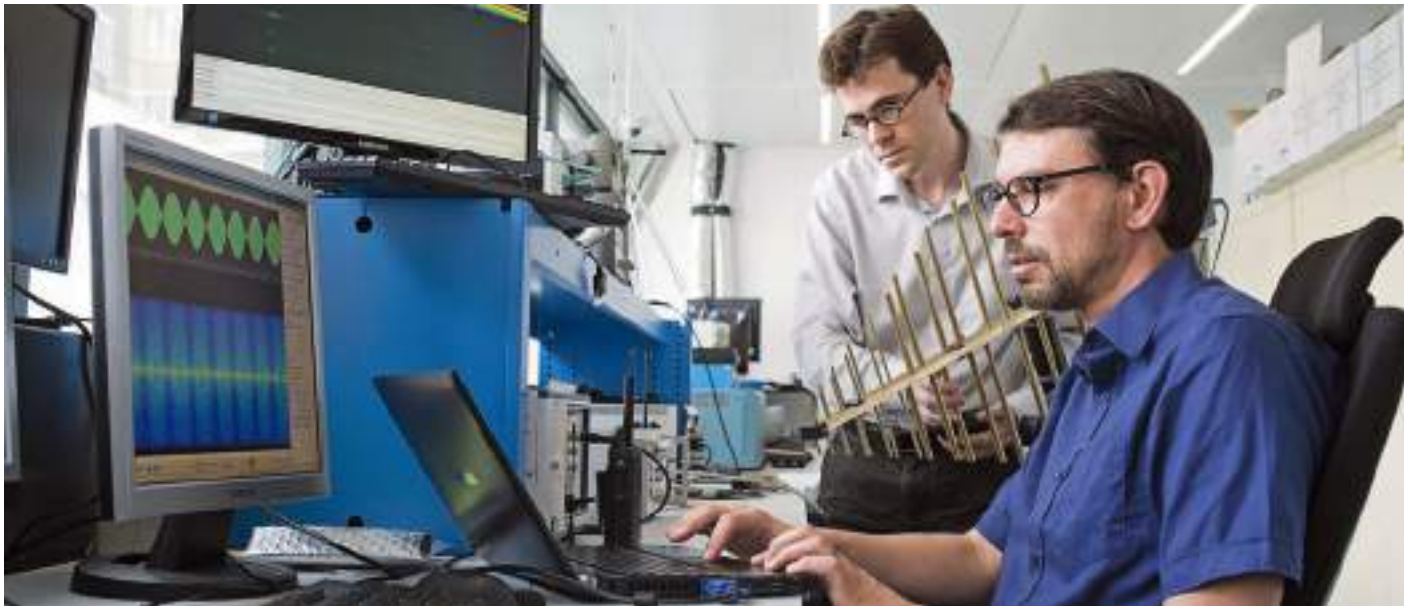
En 2016, l'agence a repensé le format du rapport pour se concentrer davantage sur l'analyse des indicateurs. La plateforme de mesure associée aux travaux de l'observatoire a, elle aussi, fait l'objet d'évolutions significatives.

Assurer la conformité aux exigences de sécurité

Dans le sillage des recommandations déjà élaborées sur la sécurité des réseaux de téléphonie mobile 2G, 3G et 4G, l'ANSSI a transmis en 2016 aux opérateurs de communications électroniques de nouvelles recommandations. Les sujets abordés : les réseaux de téléphonie mobile 4G et les services DNS *(Domain name system)* utilisés par les équipements de cœur de réseau mobile afin d'améliorer la sécurité de ces réseaux et de protéger les abonnés lors des différents cas d'itinérance.

Parallèlement, les équipes techniques de l'ANSSI ont poursuivi les actions engagées destinées à mieux appréhender les enjeux de sécurité liés à la virtualisation croissante des fonctions de cœur de réseau. Dans cette perspective, des campagnes de tests ont été menées pendant plusieurs semaines sur des plateformes représentatives mises à disposition par les opérateurs.

Toujours en lien avec les opérateurs, l'ANSSI a approfondi d'autres travaux sur la sécurisation des moyens d'administration des réseaux ainsi que sur la sécurisation des messageries grand public, objet d'une charte signée par la majorité des opérateurs en 2015.



SENSIBILISER LES PUBLICS AUX ENJEUX DE LA SÉCURITÉ NUMÉRIQUE

Face à la montée de la menace cyber, la prise de conscience du risque par les décideurs et l'ensemble de la population constitue un enjeu majeur. Dans cette optique, l'ANSSI développe une action multiforme de sensibilisation des publics.

UN DIALOGUE **DE PROXIMITÉ**

La sécurité des systèmes d'information a longtemps été perçue comme un sujet de spécialistes. Mais la multiplication et la médiatisation des attaques ont changé la donne. Progressivement, le sujet est sorti du seul périmètre du responsable de la sécurité des systèmes d'information (RSSI) pour entrer peu à peu dans le champ de vision des décideurs, d'abord, mais aussi des particuliers. Si le processus de prise de conscience ne progresse pas au même rythme que la menace, la mission de sensibilisation que mène l'ANSSI apparaît plus que jamais d'une grande nécessité.

Hygiène informatique et pédagogie

En tant que chef de file de la sécurité du numérique en France, l'ANSSI défend une approche pédagogique, positive et ancrée dans la réalité de ses publics pour renforcer son impact et éveiller l'intérêt et les consciences sur les enjeux du numérique.

En 2016, l'action de sensibilisation et de promotion des bonnes pratiques de l'agence vers l'administration, les opérateurs d'importance vitale, les responsables informatiques, les entreprises de toutes tailles ou encore les comités exécutifs s'est traduite par une communication plurielle et sur mesure. En témoignent par exemple le film *L'ANSSI en neuf 9#*, l'infographie « Surfez zen » ou encore le *Guide des bonnes pratiques de sécurité à bord des navires*. L'agence a par ailleurs publié une dizaine de nouvelles notes techniques portant notamment sur le protocole TLS, les systèmes d'exploitation GNU/Linux, le logiciel de chiffrement Zed!, la télé administration ou les systèmes industriels. Dans un souci permanent de maintien à l'état de l'art, plusieurs notes ont également été mises à jour.

II LA SENSIBILISATION À L'HEURE DE L'INNOVATION

Interaction et formation

Pour transmettre ses messages de sensibilisation, l'agence a exploré de nouveaux formats. Elle a ainsi produit Crypto - le webdoc', un web documentaire sur la cryptologie qui présente de manière simple et interactive les grandes lignes de cette science plusieurs fois millénaire à travers plusieurs chapitres (histoire, références culturelles, recherche, grands principes et législation).

L'ANSSI a également expérimenté un séminaire de sensibilisation et développé une application sous forme de *serious game* ayant pour objectif de sensibiliser les managers et dirigeants d'administrations et d'entreprises, PME comme grands groupes. L'enjeu est double puisqu'il s'agit à la fois de permettre aux participants d'acquérir une meilleure connaissance de la menace, mais aussi de les inciter à se lancer résolument dans des démarches de sécurisation.

2016 a aussi vu le lancement d'un projet de formation en ligne (MOOC) intitulée *SecNumacadémie,* dont l'objectif est de sensibiliser à la sécurité du numérique l'ensemble des personnes utilisant de l'informatique à titre professionnel et ce quel que soit leur métier. Après avoir rencontré un certain nombre d'acteurs, étatiques et privés, travaillant sur des projets de formations interactives, l'ANSSI a élaboré un cahier des charges visant à disposer d'une assistance pour la création et l'hébergement d'un tel programme de formation. Le marché public, lancé fin 2016, devrait permettre la mise en ligne du premier module de sensibilisation au printemps 2017.

L'action en régions

Alors que plus de la moitié des régions métropolitaines sont dotées de leur « référent SSI », un premier bilan très positif confirme la pertinence du dispositif et souligne les attentes des partenaires comme des « cibles » de l'ANSSI.

Une coopération étroite avec les services de l'État et les Régions

Les sept premiers référents déployés ont été immédiatement en mesure d'apporter l'appui d'un spécialiste de la sécurité des systèmes d'information aux actions conduites localement par tous les services de l'État impliqués dans les actions de sécurité économique.

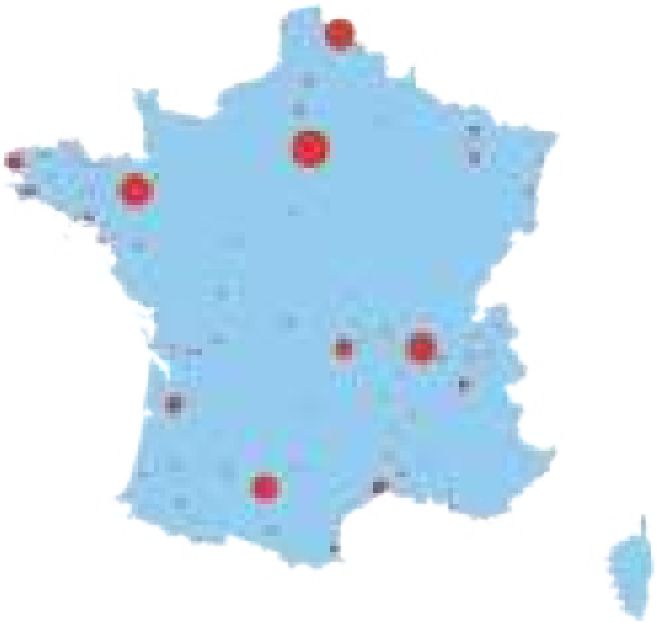
Une fois consolidée, la coopération avec les services déconcentrés de l'État est complétée par un rapprochement avec les collectivités territoriales, et tout particulièrement les Régions, compte tenu de leurs compétences en matière de développement économique. Les actions visent notamment à une meilleure intégration des questions liées à la sécurité du numérique, en amont des grands programmes de développement, de formation et de recherche portés par les Régions.

Une action au profit des opérateurs d'importance vitale, des collectivités territoriales et des acteurs privés

La proximité des référents a permis d'établir des liens plus directs avec les opérateurs d'importance vitale implantés en régions et a permis de leur fournir une assistance adaptée dans le cadre de la mise en œuvre du dispositif de cyber sécurité prévu par le Code de la défense. Le volume des sollicitations reçues par les référents montre également une attente très forte de la part des collectivités territoriales et des acteurs privés, qu'il s'agisse des entreprises (notamment les TPE/PME), des professions libérales ou des associations.

Toutes les régions métropolitaines devraient être dotées d'un référent d'ici fin 2017.

www.ssi.gouv.fr/actualite/crypto-le-webdoc



Nombre d'interventions des référents en région

PRÉSENCE MÉDIATIQUE

WEB

74
brèves en français

17
en anglais

10
nouvelles rubriques (recrutement, actions de l'agence, protection des OIV, règlement eIDAS…)

2 MARS 2016
l'ANSSI lance la version anglaise de son site web

PRESSE

234
sollicitations presse

72
interviews effectuées par la direction et les experts

4
conférences de presse thématiques

RÉSEAUX SOCIAUX

4 août 2016 l'ANSSI fête son

10 000e

abonné sur Twitter avec une surprise à la clé : le *papertoy* RIC !

Sur LinkedIn depuis la rentrée, l'ANSSI enregistrait déjà en décembre

10 575
abonnés

26
vidéos en ligne sur Dailymotion

ÉVÉNEMENTS

Participation de l'ANSSI à

140

événements en France et à l'étranger (conférences, salons…)

FORMER ET CULTIVER L'EXCELLENCE

La formation en matière de sécurité numérique est un enjeu majeur qui constitue un axe à part entière de la Stratégie nationale pour la sécurité du numérique. Dans ce cadre, l'ANSSI dispense et participe à l'émergence d'une offre de formation complète et attractive.

I CONSTRUIRE UNE CULTURE DU NUMÉRIQUE, FORMER LES EXPERTS DE DEMAIN

L'action de l'ANSSI dans ce domaine passe à la fois par la délivrance de formations spécialisées dans ses murs et par le développement de ses relations avec les organismes nationaux de formation. Les contenus pédagogiques élaborés par l'agence satisfont différents besoins allant de la sensibilisation des non-informaticiens à l'approfondissement des connaissances des spécialistes, en passant par l'initiation des informaticiens non spécialisés.

Formation interne

Tout au long de l'année 2016, le Centre de formation à la sécurité des systèmes d'information (CFSSI) a assuré des formations courtes sur un ensemble de thématiques : cryptographie, analyse de risque, audit de sécurité, etc. Ce sont ainsi 1699 chercheurs, principalement issus de l'administration, qui ont été accueillis à l'ANSSI.
Le CFSSI dispense également une formation longue sur treize mois débouchant sur la délivrance d'un titre d'« Expert en sécurité des systèmes d'information » (SSI) équivalant à un bac + 5. En 2016, 21 personnes se sont vues attribuer ce titre.

CyberÉdu à l'heure du déploiement

Lancé par l'ANSSI en 2013, le projet CyberÉdu promeut l'intégration de la sécurité numérique dans les formations supérieures en informatique non spécialisées en SSI par la fourniture de contenus pédagogiques remis aux enseignants. Ceux-ci ont été réalisés dans le cadre d'un marché passé avec l'université européenne de Bretagne et Orange. S'ajoute à cela l'organisation par le CFSSI de colloques d'accompagnement des enseignants autour des méthodes d'intégration de la sécurité dans les formations. Enfin, 2016 a vu la création d'une association qui a pris le relais de l'ANSSI sur le pilotage du projet, et un groupe de travail a été constitué en vue de l'élaboration d'un dispositif de labellisation.

II ATTIRER LES TALENTS ET CULTIVER LES COMPÉTENCES

Pour accomplir ses missions, l'ANSSI doit faire preuve d'agilité et de créativité afin d'attirer de nombreux profils aux compétences souvent très spécifiques : cryptographes, veilleurs, analystes de la menace, architectes, administrateurs réseaux, chercheurs, etc. Elle mène des campagnes de recrutement qui se manifestent par le recours aux réseaux sociaux (Twitter, LinkedIn), de fréquentes participations aux manifestations étudiantes et professionnelles ou encore l'organisation de *job datings*, dans l'objectif permanent de s'entourer des meilleurs et de faire prospérer le goût du challenge et l'émulation intellectuelle qui animent l'agence.

Côté formation, l'ANSSI s'attache à entretenir un environnement professionnel enrichissant et motivant en identifiant de manière précise les compétences attachées à chaque poste et les actions nécessaires pour accompagner les agents dans l'acquisition de celles qui pourraient leur manquer. En 2016, ce ne sont pas moins de 14500 heures de formation qui ont été dispensées, soit en moyenne 29 heures de formation par agent. Un dispositif spécifique au management a par ailleurs été mis en place afin de favoriser la construction d'une culture managériale commune, l'équilibre entre la posture d'expert et le rôle de manager et la mise à niveau des compétences.

SecNum*edu*, UN LABEL MADE IN ANSSI

PASCAL CHOUR, chargé de mission au CFSSI

« Un des moyens retenu par l'ANSSI pour améliorer l'attractivité de la filière sécurité consiste à labelliser les formations du domaine et à les mettre en avant sur notre site Internet.
En février 2016, un groupe de travail sous l'égide de l'ANSSI et comportant des industriels, des établissements d'enseignement et le MENESR a été constitué pour créer le référentiel de labellisation des formations de l'enseignement supérieur. Au printemps 2016, ce travail collectif a donné naissance au label "SecNum*edu*", qui s'adresse à des formations spécialisées dans la sécurité numérique de niveau bac + 3 à bac + 6. Ce référentiel a été présenté aux établissements fin mai 2016 pour commentaires et publié en version applicable fin juillet 2016. Les 26 premiers labels ont été remis par Guillaume Poupard aux responsables des formations lors du FIC 2017, ce qui représente plus de 750 élèves par an. L'ANSSI estime que 60 formations françaises pourraient être labellisées à terme. »

Une politique de ressources humaines pour l'ANSSI a été adoptée au premier semestre 2016. Elle repose sur le renforcement de l'attractivité de l'agence et la fidélisation de ses agents, l'optimisation de la gestion des ressources humaines et l'amélioration de la lisibilité et de la cohérence des parcours professionnels.

"En matière de recrutement, le niveau d'exigence de l'ANSSI est très élevé, qu'il s'agisse de compétences ou d'éthique. Habilités secret-défense, nos agents ont le sens du devoir et le goût de servir la Nation."

Guillaume Poupard

UNE AGENCE D'EXPERTISE SCIENTIFIQUE

Pour l'ANSSI, la recherche est une nécessité absolue. Elle dispose aujourd'hui de six laboratoires spécialisés en sécurité des composants, des technologies sans fil, des systèmes embarqués, des réseaux et protocoles, ainsi qu'en technologies de détection et en cryptographie. Par leurs activités de recherche souvent conjointes, les 58 chercheurs de la division scientifique et technique nourrissent les travaux des autres entités de l'agence et ses réflexions sur les sujets émergents *(blockchain)*. Parmi les programmes clés de l'année 2016 figurent notamment la cryptographie dite « post-quantique », les objets connectés ou encore les agressions électromagnétiques intentionnelles.

L'ANSSI est par ailleurs très impliquée dans l'orientation et le suivi des différents appels à projet visant à financer la recherche scientifique ou la R&D industrielle, en lien notamment avec l'Agence nationale pour la recherche (ANR) et le Commissariat général à l'investissement. Ses laboratoires sont engagés dans plus d'une dizaine de projets de recherche collaboratifs conduits sous l'égide de l'ANR ou dans le cadre du programme européen Horizon 2020.

Acteurs majeurs du rayonnement scientifique de l'ANSSI, les membres de la division scientifique et technique contribuent activement à la recherche académique par de nombreuses publications (45 en 2016) dans des conférences et revues prestigieuses du domaine de la SSI.

Chaouki Kasmi,

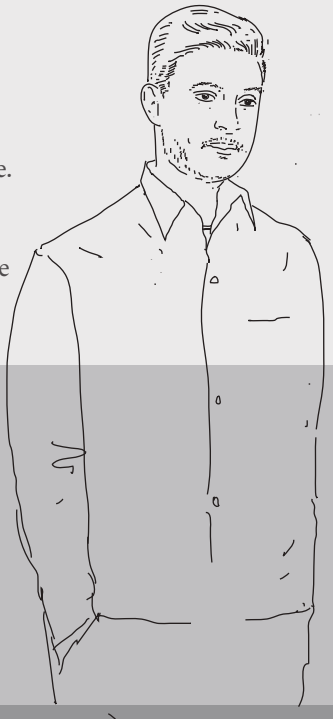
chercheur en sécurité électromagnétique

« Au sein de l'ANSSI, je m'intéresse aux interférences électromagnétiques intentionnelles (bruit, vecteurs champs forts…) qui menacent l'intégrité et la disponibilité des systèmes. Les derniers travaux ont permis de démontrer qu'il était possible de prendre le contrôle d'un smartphone par injection de commandes vocales à distance. »

LE PROFIL

Adolescent, Chaouki Kasmi faisait des expériences avec son micro-ondes. Il réalisait des « tests » dans son garage.

Chaouki a intégré l'ANSSI en 2009, on le surnomme le « Chercheur touche à tout ».



Aujourd'hui, Chaouki est adjoint du laboratoire sécurité des technologies sans fil, auteur d'une soixantaine d'articles, dont plusieurs primés. Il est lauréat de deux *Young Scientist Awards* de l'URSI et d'un titre de *Life Fellow* décerné par la fondation Summa.

AU CŒUR DE LA RECHERCHE

« Ce décloisonnement entre la recherche fondamentale et l'action concrète est l'un des aspects les plus passionnants de la mission de chercheur au sein de l'ANSSI. »

- Avec les autres chercheurs de son laboratoire, Chaouki mène de nombreuses prestations d'audit et de durcissement de sites.
- Il participe à la rédaction des réglementations de l'UE et de l'Otan.
- Encore émergente ces dernières années, la sécurité électromagnétique est devenue un sujet stratégique pour la SSI.

LES COMPÉTENCES

Cyber sécurité
Gestion des risques
Cryptographie
Traitement de signal
Sécurité électromagnétique
Biométrie

FAVORISER UN ÉCOSYSTÈME DE CONFIANCE : INCUBER ET COOPÉRER

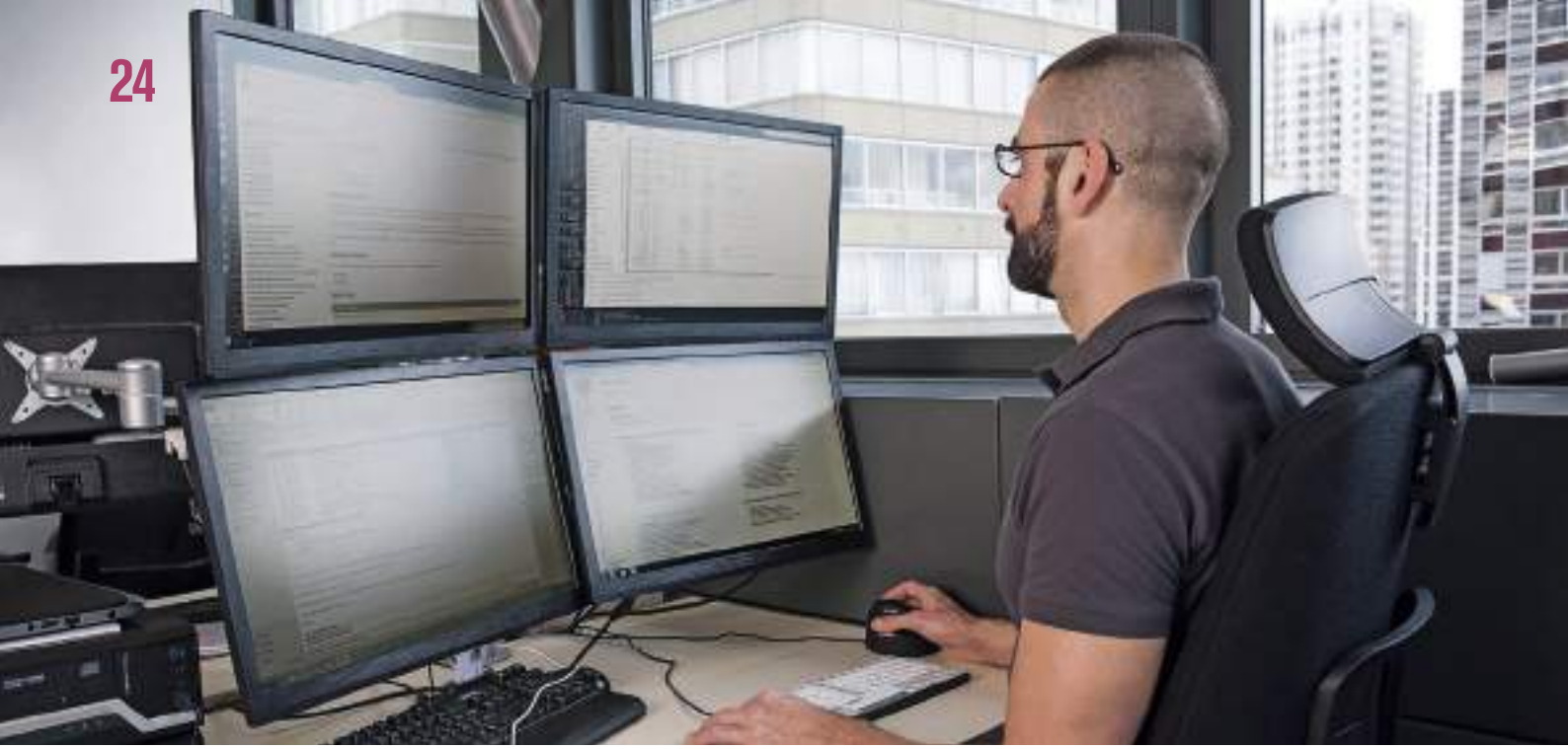
La révolution numérique oblige à revoir les modèles de gouvernance. Agence experte et agile, l'ANSSI s'attache à créer les conditions d'une sécurisation globale du cyber espace en conjuguant sensibilisation et développement du tissu industriel. Elle utilise pour y parvenir tous les leviers à sa disposition : coopération interministérielle, territoriale, qualification et certification, mais aussi incubation, etc.

COOPÉRATIONS À L'ÉCHELLE INTERMINISTÉRIELLE

À la fois agence interministérielle et autorité nationale, l'ANSSI est par nature en relation directe avec les différentes entités qui traitent des questions cyber au sein des ministères de l'Intérieur, de la Défense, de l'Économie et des Finances et celui des Affaires étrangères et du développement international, avec lesquelles elle coopère régulièrement en apportant son expertise et son assistance technique et réglementaire.

L'agence travaille également en étroite collaboration avec la Direction interministérielle du numérique et des systèmes d'information et de communication (Dinsic) autour des grands projets SI de l'État, à l'instar de France connect, du *cloud* étatique ou du programme Ensap, qui vise à créer un espace numérique sécurisé à l'intention des agents publics.

Par ailleurs, en cette année 2016 largement placée sous le signe de la loi de programmation militaire, l'ANSSI a activement poursuivi ses interactions avec les hauts fonctionnaires de défense et sécurité et les branches métiers des différents ministères de tutelle en charge des activités d'importance vitale. Les coordinateurs territoriaux ont quant à eux poursuivi leur collaboration avec les différents acteurs locaux (préfectures, agents du ministère de l'Intérieur et du ministère de la Défense) afin de délivrer un message unique de sensibilisation aux publics identifiés. Cette politique de coopérations directes s'est également concrétisée sur le terrain, notamment auprès des gendarmes et des policiers dans le cadre du processus de transformation numérique des forces de l'ordre (programmes NÉOgend et NÉOpol, *voir p. 28*).



UNE DÉMULTIPLICATION DE L'EXPERTISE

Parce qu'une seule agence – même forte de 500 collaborateurs – ne peut pas, à elle seule, répondre aux besoins de tout un pays en matière de cyber sécurité, l'ANSSI s'est engagée depuis plusieurs années dans la construction d'un écosystème réunissant, au sein d'un même catalogue, de nombreux services de confiance dans les différents métiers concourant à la sécurité numérique.

Qualification de produits et de prestataires de confiance

L'ANSSI développe une politique de labellisation de produits et services de sécurité ambitieuse. En 2016, un travail de fond considérable d'unification des processus de qualification issus des différents cadres réglementaires (référentiel général de sécurité – RGS, loi de programmation militaire – LPM, et règlement européen – eIDAS) a été mené. Devant aboutir en 2017, il a d'ores et déjà permis de mettre en œuvre des procédures visant à améliorer le suivi dans la durée des produits qualifiés, de leurs évolutions fonctionnelles et de leur niveau de sécurité.

Un effort particulier a également été consacré à l'élaboration d'une méthodologie de qualification de sondes de détection d'attaques informatiques, type de produits qui n'a jusqu'à présent jamais été labellisé par l'ANSSI, mais dont la mise en œuvre par les OIV sera à terme obligatoire au titre des nouvelles dispositions introduites par la loi de programmation militaire de 2013. Ces travaux ont débouché sur un cadre d'évaluation qui sera expérimenté au cours d'évaluations pilotes lancées fin 2016.

17
processus de qualification de prestataires d'audit en sécurité des systèmes d'information engagés

5
prestataires en cours de qualification dans chaque secteur suite au lancement de qualification des prestataires de réponse à incident de sécurité (PRIS) et des prestataires de détection d'incident de sécurité (PDIS)

1
référentiel *SecNumCloud Essentiel* destiné aux prestataires d'informatique en nuage

22
nouvelles qualifications de prestataires d'audit en sécurité des systèmes d'information (PASSI)

L'ANSSI a qualifié 16 nouveaux produits et accordé 13 agréments pour la protection d'informations sensibles ou classifiées. Au-delà de ces labels ayant la portée de recommandations d'usage, le centre de certification de l'agence a quant à lui certifié 95 produits.

INCUBER
LES PROJETS DE DEMAIN

Labelliser, qualifier, certifier… C'est bien. Mais depuis quelques années, l'ANSSI a décidé de s'inscrire plus en amont encore dans la chaîne de valeur de la sécurité numérique. En adoptant une posture d'incubateur, l'agence façonne et encourage des projets innovants qui participent à l'établissement d'un environnement de confiance avant de les laisser prendre leur autonomie. Après le programme CyberÉdu, centré sur l'intégration de la thématique de la sécurité numérique dans les formations en informatique non spécialisées *(voir pages précédentes)*, l'ANSSI s'est engagée en 2016 dans le chantier de préfiguration d'une plateforme d'assistance aux victimes d'actes de cyber malveillance (ACYMA) destinée aux particuliers, aux entreprises et aux administrations en vue du déploiement d'une plateforme numérique en 2017.

Paroles d'acteurs

Jérôme Notin,

chef du projet ACYMA

UN DISPOSITIF NATIONAL « La Stratégie numérique du gouvernement lancée en juin 2015 a engagé la mise en place du dispositif national d'assistance aux victimes d'actes de cyber malveillance. Afin de définir le périmètre du projet, un groupe de travail, copiloté par l'ANSSI et le ministère de l'Intérieur, a été mis en place et a rendu ses conclusions en avril 2016. »

TROIS MISSIONS MAJEURES POUR UN PUBLIC COMPLÉMENTAIRE À CELUI DE L'AGENCE « La première mission du dispositif est l'assistance de proximité. Chaque victime pourra ainsi être mise en relation, à travers une plateforme web, avec un prestataire référencé. La mise en place de campagnes de prévention et de sensibilisation est également prévue par le dispositif afin de diffuser les bonnes pratiques en matière de sécurité numérique. Enfin, la troisième mission est de mettre en place un observatoire de la menace numérique. En complément des statistiques, cet observatoire offrira une vue réelle et consolidée de la menace afin de mieux l'anticiper. Le public visé concerne les particuliers, les entreprises et les collectivités qui ne sont pas gérés par l'agence. »

UN PROJET INCUBÉ AU SEIN MÊME DE L'ANSSI « L'agence a mis en place dès la mi-2016 une équipe projet afin d'incuber le dispositif. J'ai ainsi pu m'appuyer sur les conclusions du groupe de travail initial pour mener le travail opérationnel et les choix de structure. Il s'agissait de bénéficier de l'expertise de l'agence sur certains services – juridiques, techniques, administratifs et communication – afin de travailler sur les modalités de création et de fonctionnement du dispositif. C'est ce travail préparatoire de fond réalisé par l'ANSSI qui va nous donner les moyens de passer en 2017 à la création d'un groupement d'intérêt public (GIP) qui nous permettra de disposer d'une certaine indépendance de fonctionnement, tout en conservant des liens très étroits avec l'administration, et en particulier l'agence. »

Le dispositif doit voir le jour mi-2017 sous la forme d'une plateforme numérique : cybermalveillance.gouv.fr, avec une première phase pilote dans la région des Hauts-de-France.

2. GARANTIR LA SOUVERAINE NATIONALE

12
secteurs d'activité d'importance vitale

450 000
postes chiffrés

2 140
marqueurs techniques

TÉ

La lutte contre le terrorisme, mais aussi l'urgente nécessité de protéger les intérêts de la Nation comme les droits et libertés des citoyens appellent une prise de conscience nouvelle sur les enjeux liés à l'exercice de la souveraineté de la France dans le domaine du numérique. Mais comment défendre nos positions dans ce nouveau terrain de jeu géopolitique aux frontières poreuses et mouvantes ? Au fil des ans, l'ANSSI développe des réponses de plus en plus efficaces, évolutives et collaboratives pour assurer la sécurité de l'État et celle des opérateurs d'importance vitale.

SOUTIEN ET SÉCURITÉ DE L'ÉTAT

Autorité nationale en matière de sécurité des systèmes d'information, l'ANSSI est le garant d'une prise en compte coordonnée, ambitieuse et volontariste des questions de cyber sécurité en France. Au quotidien, ses différentes activités concourent à assurer la continuité du fonctionnement régalien et à préserver les intérêts de la Nation.

L'ANSSI, GARANTE DE LA **SÉCURITÉ DES COMMUNICATIONS DE L'ÉTAT**

Afin d'assurer la sécurité des communications des plus hautes autorités de l'État et des ministères, y compris les plus sensibles, l'ANSSI conçoit, développe, évalue et met en œuvre une large gamme de produits et de services interministériels sécurisés. Pour les sous-directions Expertise (SDE) et Systèmes d'information sécurisés (SIS), il s'agit d'un double challenge puisque les solutions développées doivent à la fois être ergonomiques et à l'état de l'art en matière de sécurité. 2016 a notamment été marquée par l'aboutissement d'un programme de développement majeur qui a contribué à l'élaboration d'une nouvelle offre de téléphonie fixe sécurisée.

Après Isis et Horus, voici Osiris

Sur la base de réflexions stratégiques menées en 2015, la sous-direction SIS a engagé en début d'année un important programme de définition de la solution et d'identification des produits. Au second semestre, cette première phase a débouché sur le lancement de la construction de l'infrastructure définitive. Un chantier imposant, tant par le défi technologique qu'il représente que par son calendrier serré et la multiplicité des acteurs à coordonner. Baptisé Osiris, le dispositif, compatible avec le téléphone chiffré Teorem, assurera les transmissions qui relèvent du secret de la défense nationale. Il sera mis en service à partir du second trimestre 2017 pour l'arrivée des nouvelles équipes gouvernementales.

En parallèle, dans le cadre du processus d'amélioration continue de l'intranet interministériel Isis, les équipes de SIS ont entrepris des travaux de stabilisation du système permettant de conserver un niveau de disponibilité toujours adapté aux contraintes d'utilisation. La sous-direction a également poursuivi le déploiement de la solution de visioconférence Horus dans différentes entités ministérielles et apporté son soutien au Centre de transmission gouvernemental dans la mise en place de plusieurs liaisons avec des partenaires étrangers, répondant ainsi aux besoins des plus hautes autorités de l'État.

Les forces de l'ordre équipées de Secdroid

Le programme Secdroid (système d'exploitation pour terminaux mobile) a, quant à lui, continué à être déployé au sein du SGDSN et de l'ANSSI, au ministère de la Justice ainsi que dans la Gendarmerie et la Police nationale dans le cadre des programmes NÉOgend et NÉOpol. Ces derniers visent à équiper les gendarmes – et à plus long terme les policiers – de smartphones et tablettes pour promouvoir une nouvelle forme de proximité avec la population. En 2016, après un premier pilote dans les Hauts-de-France, les gendarmes de Bourgogne-Franche-Comté ont pu tester le dispositif (1 150 gendarmes équipés), qui sera déployé à l'ensemble des unités de gendarmerie, soit 60 000 gendarmes, d'ici à la fin 2017.

450 000 postes chiffrés

Investie dans la sécurisation des moyens de communication, l'ANSSI est aussi en charge du déploiement de produits de confiance au sein de l'administration ministérielle. En 2016, plus de 450 000 postes informatiques ont été équipés de produits de chiffrement qualifiés de l'éditeur Prim'x, auprès de qui l'ANSSI avait acquis une licence globale libératoire en 2015. Parallèlement, un nouveau projet a été initié, en lien étroit avec la Direction interministérielle du numérique et des systèmes d'information et de communication (Dinsic), pour équiper à partir de 2017 l'ensemble des cabinets ministériels et de leurs interlocuteurs directs au sein des administrations en solutions compatibles de téléphonie mobile sécurisée.

UN ACTEUR CLÉ DES GRANDS PROJETS NUMÉRIQUES DE L'ÉTAT

SECDROID

OSIRIS

HORUS

ISIS

Analyser les risques, proposer une assistance technique grâce à ses experts mais aussi déployer des produits de confiance constitue une part importante de l'activité de l'ANSSI.

17 000

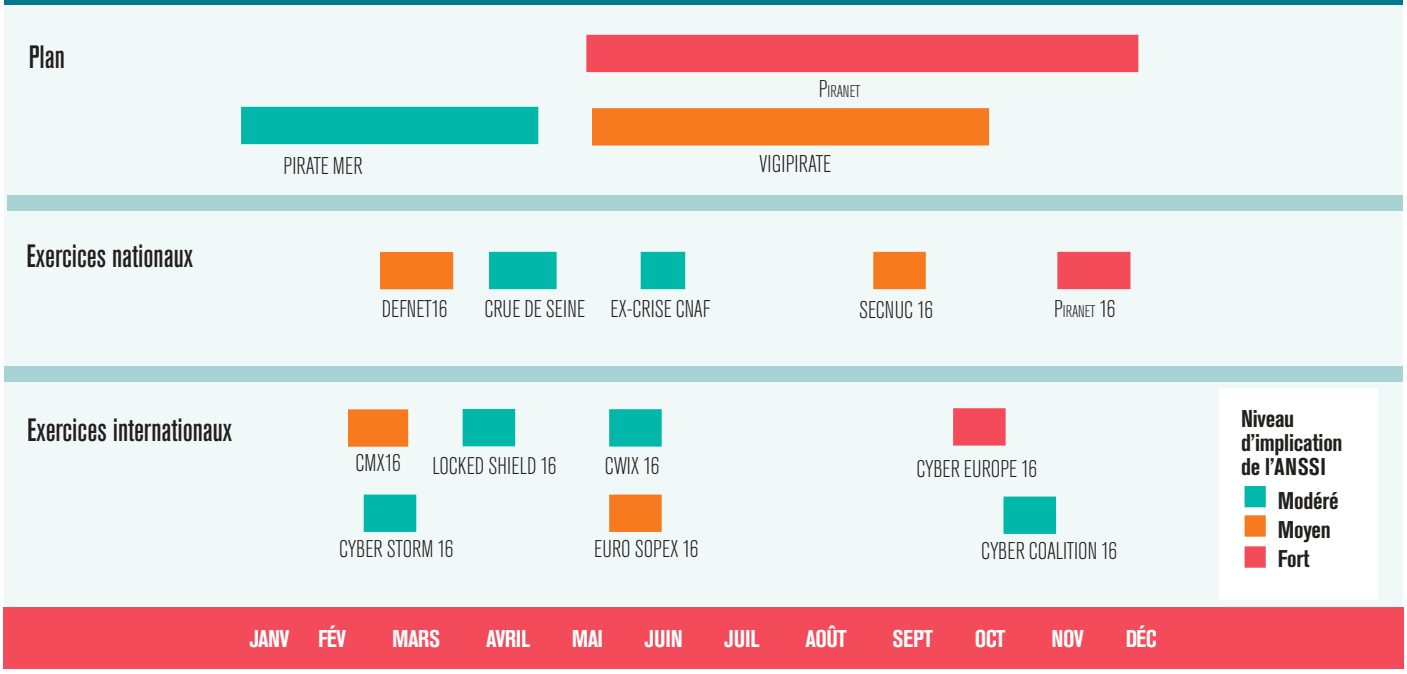
sites sécurisés d'ici à la fin de l'année 2017

Plusieurs projets importants ont rythmé l'année 2016, à l'instar du chantier de sécurisation et d'urbanisation du réseau interministériel de l'État (RIE), des projets interministériels d'informatique en nuage ou encore de la solution d'identification et d'authentification France Connect.

AU CŒUR DU DISPOSITIF DE CRISE DE L'ÉTAT

Quelles que soient les circonstances, dans le cadre d'un grand événement planifié ou inopiné, en cas d'urgence ou de force majeure, l'ANSSI met sur pied un dispositif agile de gestion de crise cyber, destiné à apporter une réponse adaptée et coordonnée entre tous les acteurs concernés. Dans ce cadre, l'agence assure la corrélation et la synthèse des informations liées à la sécurité numérique fournies par les ministères, en plus des données produites par ses propres moyens. De son côté, en lien avec la sous-direction RELEC, chargée de la communication de crise, des relations interministérielles et sectorielles, le COSSI établit différents points de situation, notes de synthèses et dossiers d'anticipation de la menace – permettant d'apprécier l'ampleur des développements de chaque événement dans le cyber espace –, qu'il a transmis à la Cellule interministérielle de crise (CIC).

Planification des risques en 2016, l'ANSSI en permanence en anticipation de la crise



UN "STRESS TEST" POUR LE PLAN PIRANET

Samuel Hassine, chargé de mission au sein du pôle Planification, Exercice et Gestion de crise (RELEC)

« Le plan PIRANET est un plan gouvernemental de la famille « Pirate » qui regroupe des plans d'intervention déclenchés par le Premier ministre en cas de menaces avérées ou d'attaques majeures. Élaboré il y a une quinzaine d'années et centré sur la cyber sécurité, il a fait l'objet, entre 2014 et 2016, d'une refonte en vue de l'adapter aux impératifs et aux innovations de ce domaine en constante évolution. Chaque fois qu'un plan d'une telle importance est revu en profondeur, le SGDSN planifie et conduit un exercice majeur de niveau stratégique (impliquant les hautes autorités de l'ensemble des ministères) afin de valider à la fois ses différents axes, la pertinence des dispositifs de gestion de crise qu'il décrit et, plus généralement, la capacité de l'État à se coordonner pour faire face à des attaques informatiques de grande ampleur. L'exercice PIRANET 16 s'est déroulé du 6 au 8 décembre, mobilisant au total plus de 170 agents issus des ministères et d'OIV. Le scénario simulait une compromission massive de plusieurs systèmes d'information sensibles par un groupe d'attaquants possédant des capacités techniques avancées. Ciblant principalement le secteur de l'énergie, l'attaque s'est ensuite propagée à l'ensemble des services de l'État, incluant plusieurs administrations déconcentrées. Avec près de 40 agents de l'ANSSI mobilisés, pour certains pendant six mois, nous avons tenu un rôle majeur dans la préparation et la conduite de ce *stress test* du plan PIRANET. D'une part, nous avons élaboré le scénario technique en relation étroite avec les joueurs selon leurs objectifs respectifs et, d'autre part, nous avons mené l'animation de l'exercice et assuré sa cohérence tout au long de son déroulé. Aussi, la Cellule interministérielle de crise (CIC), armée à l'occasion de cet entraînement, a été présidée par Guillaume Poupard, directeur général de l'agence. Après un premier bilan à chaud largement positif, nous travaillons actuellement à un retour d'expérience exhaustif. »

PROTECTION ET DÉFENSE DES INTÉRÊTS VITAUX DE LA FRANCE

Pour défendre les intérêts vitaux de la Nation, l'ANSSI dispose d'une capacité de veille, de détection, d'évaluation et de défense de la menace à la pointe des technologies et en lien direct avec les hautes autorités. Des missions clés portées par le COSSI.

Au sein de l'ANSSI les agents du Centre opérationnel de la sécurité des systèmes d'information servent la mission principale de défense des systèmes d'information. Les équipes du COSSI sont chargées de détecter et d'entraver les attaques visant notamment les systèmes d'information de l'État et des opérateurs d'importance vitale. Leurs missions sont variées, allant de l'analyse des menaces et des vulnérabilités à la remédiation post-crise, en passant par la qualification des attaques en cours et la définition des mesures de réponse.

IDENTIFICATION ET ANALYSE DE **LA MENACE**

Le métier des analystes du COSSI ? Collecter, analyser et qualifier les vulnérabilités et les codes malveillants qui menacent la sécurité des systèmes d'information de l'État et des opérateurs d'importance vitale. En 2016, les équipes d'analystes de vulnérabilités et codes malveillants ont développé 7130 signatures de détection, dont 6689 ont été intégrées aux sondes supervisées par l'ANSSI. À ce titre, 2140 marqueurs techniques ont été communiqués aux ministères et aux opérateurs d'importance vitale à des fins de recherches d'éventuelles compromissions de leurs systèmes informatiques. Ces travaux ont fait l'objet de 12 rapports d'analyse de codes malveillants et de trois rapports détaillés d'analyse de vulnérabilités. En outre, 431 avis sur des correctifs de sécurité et dix alertes techniques sur des vulnérabilités critiques ou des vagues d'attaques ont été publiés sur le site du CERT-FR, assortis de propositions d'actions destinées à réduire les risques.

Les analystes du COSSI sont également en charge de l'anticipation et de l'analyse des risques et menaces, croisant et synthétisant les informations issues de sources internes et externes, et diffusant des notes de synthèse en coopération avec les équipes techniques de l'ANSSI. Ils interviennent, enfin, lors du traitement d'incidents majeurs (opérations de cyber défense), notamment pour comprendre les schémas et les modes opératoires des cyber attaques. Au total, en 2016, 649 productions ont été réalisées par les analystes des cyber menaces et les analystes en charge de la situation opérationnelle.

L'ANSSI s'engage à la plus stricte confidentialité quant à l'identité des victimes d'attaques. Elle ne recherche pas l'identité des assaillants. L'attribution – c'est-à-dire l'identification des auteurs des attaques – relève du champ judiciaire et des services du renseignement.

VEILLE ET **SUPERVISION**

À l'automne 2016, le COSSI/CERT-FR s'est doté d'un nouveau point de contact unique regroupant deux équipes installées au centre de cyber défense. La première assure la **veille et la permanence opérationnelle.** Activée 24 heures sur 24, 7 jours sur 7, 365 jours par an, elle est chargée de la réception et de la prise en compte de signalements d'événements de sécurité numérique. En 2016, elle a comptabilisé 2343 événements et transmis aux équipes d'investigation la moitié d'entre eux, les autres n'étant pas d'origine malveillante. 79 événements importants ont fait l'objet d'une alerte immédiate auprès des autorités.
Au quotidien, cette équipe est aussi responsable du suivi permanent de l'actualité mondiale en matière de cyber sécurité, produisant chaque jour une revue de l'actualité du domaine de la cyber sécurité à l'intention des agents de l'ANSSI, des services de l'État et des OIV. Près de 4500 articles ont ainsi été publiés en 2016.
La seconde équipe est dédiée à la **supervision du système de détection,** à base de sondes positionnées sur les passerelles entre les ministères et le réseau Internet. Chaque mois, plus de 2 millions d'événements sont ainsi reçus par les veilleurs supervision, qui les regroupent, les trient, les filtrent et les routent vers les équipes d'investigation.
Ainsi en 2016, l'activité de supervision a généré 512 signalements, ayant conduit à 159 traitements d'incidents, dont trois qualifiés comme critiques. Les faux positifs, quant à eux, sont transmis aux équipes d'investigation afin que ses équipes puissent affiner les marqueurs dans une optique d'amélioration continue.

L'ANSSI a effectué 20 interventions majeures auprès de grandes entreprises, principalement des OIV.

COSSI
15 MOIS AU CŒUR DE L'ACTION

2015

Un audit de l'ANSSI mené sur la bureautique et le système d'information industriel d'un opérateur d'importance vitale conclut à la vulnérabilité de l'entreprise aux attaques informatiques, même les moins sophistiquées. Il révèle en outre des traces d'activités malveillantes.

Compte tenu de ces constats, l'entreprise missionne l'ANSSI sur des analyses approfondies qui motivent l'ouverture d'une opération. Cette action, conduite au COSSI par un responsable d'opérations de cyber défense, mobilise les experts de la réponse à incidents, des auditeurs et des analystes de la menace. Les investigations confirment que l'entreprise est victime d'au moins trois attaques informatiques ciblées, les agresseurs étant parvenus à obtenir le contrôle total des systèmes d'information, dont certains pilotent des activités industrielles. Face à la gravité de la situation, les mesures techniques appliquées en urgence ne suffisent pas. L'enjeu est de convaincre les décideurs d'augmenter significativement le niveau de sécurité de l'entreprise vis-à-vis de la menace. À cet effet, le COSSI prépare avec le RSSI la sensibilisation du comité exécutif.

Au cours d'une rencontre avec la direction de l'ANSSI, les dirigeants de l'entreprise prennent conscience des risques encourus et actent le démarrage d'un vaste projet de sécurisation des systèmes d'information.

2016

Le COSSI accompagne l'entreprise et les prestataires dont elle s'est entourée dans la mise en œuvre d'un plan d'action visant la reprise de contrôle du système d'information.

Satisfait du niveau d'autonomie acquis par l'entreprise, le COSSI passe le relais aux sous-directions RELEC (Relations extérieures et Coordination) et SDE (Expertise) pour un suivi à long terme.

PLUS DE **SYNERGIES** ENTRE SUPERVISION ET VEILLE

JEAN-LOUIS DAUX, chef de bureau Supervision et Veille

« Le rapprochement des équipes chargées de la supervision et de la veille au sein d'un même bureau a permis de générer des synergies qui viennent faciliter et enrichir les missions de chacun. Ainsi, quand un agent de la veille reçoit un signalement ou détecte un site indisponible, il peut s'adresser à l'un de ses collègues chargé de la supervision pour qu'il cherche des traces de l'événement parmi les informations transmises par les sondes. À l'inverse, la revue de presse de l'équipe de veille peut attirer l'attention de la supervision sur certaines menaces. C'est ce qui s'est passé à l'apparition du *malware* Mirai, qui fit rage durant l'automne 2016. »

L'ANSSI peut désormais protéger l'identité de ceux qui signalent des failles ou des vulnérabilités.

L'article 47 de la Loi pour la république numérique du 7 octobre 2016 donne un cadre à l'agence pour réaliser les activités techniques nécessaires à la qualification des signalements. Sur les trois derniers mois de 2016, l'ANSSI a ainsi reçu une soixantaine de déclarations permettant d'identifier plusieurs vulnérabilités concernant des systèmes sensibles.

PROTÉGER LES ENTREPRISES DE LA MENACE CYBER

Protection des systèmes d'information les plus sensibles, mise en place de règles de sécurité, accompagnement, intervention en cas d'attaque… Dans le cadre de la loi de programmation militaire (LPM), l'ANSSI joue un rôle clé dans la défense des opérateurs d'importance vitale. Une autre facette de son activité consiste à développer des partenariats industriels dans le cadre du plan Cyber Sécurité de la Nouvelle France industrielle.

L'ANSSI AUX CÔTÉS DES OIV

En 2015, le cadre réglementaire dans lequel s'inscrit la mission de l'ANSSI a évolué avec la parution de décrets d'application de la loi de programmation militaire 2014-2019 relatifs à la sécurité des systèmes d'information des opérateurs d'importance vitale. L'agence s'est ainsi vu conférer de nouvelles prérogatives. Au nom du Premier ministre, elle peut désormais imposer des mesures de sécurité aux OIV et contrôler ou faire contrôler leurs systèmes d'information les plus critiques. Afin que les objectifs fixés par la loi puissent être atteints, il était nécessaire de les affiner en fonction des caractéristiques et des contraintes propres aux secteurs d'activité des OIV. Au sein de l'ANSSI, c'est le bureau Coordination sectorielle (COS) rattaché à la sous-direction Relations extérieures et Coordination (RELEC) qui pilote ce chantier, en coopération opérationnelle avec le Centre opérationnel de la SSI (COSSI) et la sous-direction Expertise (SDE).

Plus de 60 réunions et neuf arrêtés

Dès 2014, les coordinateurs sectoriels ont monté des groupes de travail réunissant les ministères concernés et les OIV dans le but de définir des règles de sécurité les plus efficaces et les plus adaptées. En 2016, ces travaux ont abouti à la parution de neuf premiers arrêtés sectoriels. Lors de l'entrée en vigueur des arrêtés les concernant, les OIV sont tenus de déclarer à l'ANSSI leurs incidents de sécurité et de mettre en place les 20 règles de sécurité définies par l'ANSSI. Dans un délai de trois mois, ils doivent également avoir identifié et déclaré leurs systèmes d'information d'importance vitale.

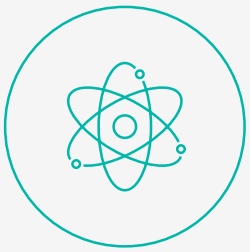
Le coordinateur sectoriel, un interlocuteur privilégié pour les OIV et les ministères

Le bureau Coordination sectorielle (COS), au sein de la sous-direction Relations extérieures et Coordination (RELEC) de l'ANSSI, compte une quinzaine de coordinateurs, dotés d'une solide culture SSI et d'une connaissance approfondie des secteurs et ministères dont ils ont la charge. Interface privilégiée des OIV et ministères, le coordinateur sectoriel pilote auprès des opérateurs de son portefeuille les actions de l'agence en les structurant autour d'une stratégie qu'il a la responsabilité d'établir. Dans ce cadre, il est amené à assurer de multiples travaux et arbitrages, instruit notamment les demandes d'assistance technique ou d'audit, et suit l'application des recommandations formulées à leur issue. Le coordinateur sectoriel joue également un rôle important dans la sensibilisation des opérateurs aux problématiques de cyber sécurité.

Enfin, le bureau COS s'investit dans la mise en œuvre d'un cadre réglementaire adéquat pour assurer le renforcement de la cyber sécurité de ces opérateurs.

En 2016, il a ainsi piloté d'importants chantiers de déclinaison sectorielle des dispositions de l'article 22 de la LPM, poursuivis par un travail tout aussi conséquent d'analyse des premières vagues de déclaration de systèmes d'information d'importance vitale (SIIV) transmis par les OIV dans le cadre de la mise en œuvre de ces dispositions.

Les **12 secteurs** d'activité d'importance vitale



SECTEURS DE LA VIE ÉCONOMIQUE ET SOCIALE DE LA NATION

Énergie, communications électroniques, audiovisuel et information, transports, finances, industrie

SECTEURS ÉTATIQUES

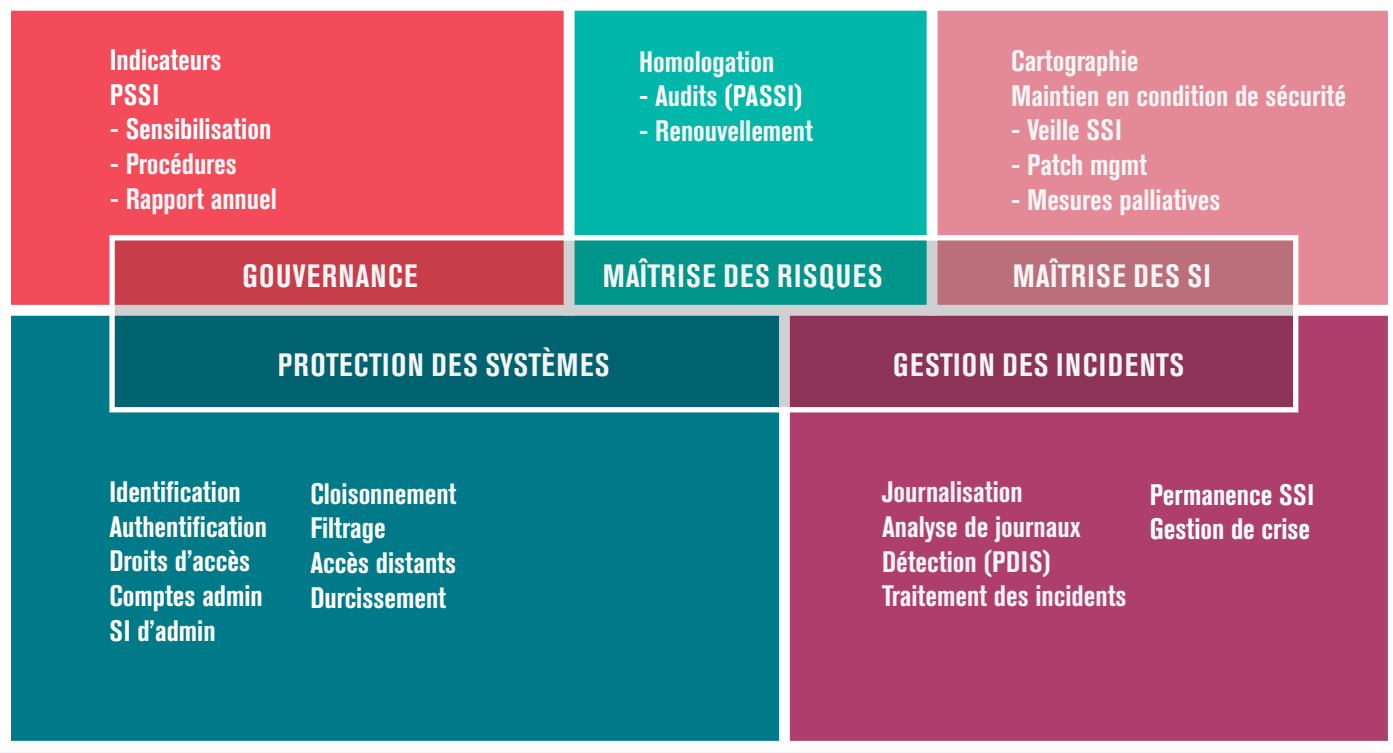
Activités civiles de l'État, activités militaires de l'État, activités judiciaires, espace et recherche

SECTEURS DE LA PROTECTION DES CITOYENS

Santé, gestion de l'eau, alimentation

Au total, la liste des OIV comporte plus de 230 organisations. Neuf arrêtés sectoriels ont été publiés en 2016 – dont trois distincts pour le secteur des transports – et quatre autres sont parus en janvier 2017.

LES 20 RÈGLES
DE LA LOI DE PROGRAMMATION MILITAIRE



UN MOTEUR DE L'INDUSTRIE DE LA SÉCURITÉ NUMÉRIQUE

Le 12 septembre 2013, le président de la République et le ministre de l'Économie, de l'Industrie et du Numérique lançaient les 34 plans de la Nouvelle France industrielle (NFI). Confié à l'ANSSI, le 33e plan de ce dispositif porte sur la cyber sécurité, avec l'objectif de développer une industrie performante pour répondre aux enjeux de souveraineté et instaurer une véritable confiance numérique dans le pays. Il s'organise autour de quatre axes : l'accroissement de la demande en solutions de cyber sécurité de confiance, le développement d'offres de confiance, l'organisation de la conquête des marchés à l'étranger et, enfin, le renforcement des entreprises nationales du domaine cyber sécurité. L'une des actions prioritaires de ce plan est le label France Cybersecurity, destiné à identifier les offres nationales et à en faire un gage de qualité et de performance. Lancé en janvier 2015, ce label a d'ores et déjà été décerné à 77 entreprises, dont 41 en 2016. Parallèlement, l'agence a poursuivi la mise en œuvre d'autres volets du plan Cyber Sécurité. Elle a notamment contribué à l'élaboration d'une feuille de route relative à l'Internet des objets et mis en place un groupe de travail sur l'élaboration d'un observatoire national de la sécurité du numérique. De leur côté, les équipes de l'ANSSI en charge de la politique industrielle ont conduit environ 300 entretiens bilatéraux avec des entreprises du secteur de la sécurité numérique afin de parfaire leur connaissance du paysage économique, des besoins et de l'offre.

Soutien à l'accès au financement

Des synergies ont été créées en 2016 avec de nombreux fonds d'investissement privés et ont permis une meilleure rencontre entre l'offre de financement et les entrepreneurs de la cyber sécurité.
Par ailleurs, la convention avec Bpifrance qui permet de soutenir l'innovation et la croissance dans les PME a été renouvelée en 2016 et son périmètre d'action a été élargi.

Paroles d'acteurs

Bernard Lassus,

directeur du programme LINKY pour ENEDIS

EXEMPLE DE PARTENARIAT INDUSTRIEL « ENEDIS prévoit, à travers son programme LINKY, d'installer 35 millions d'objets connectés dans les foyers français d'ici 2021 : des compteurs d'énergie communicants. Cela signifie que nos compteurs peuvent recevoir des ordres et envoyer des données sans intervention physique d'un technicien. Un système prévu pour faciliter la vie de nos clients, mais aussi un vrai challenge industriel en pleine explosion de la cyber menace. »

UNE SÉCURISATION MAXIMUM « Dès la genèse du projet, nous sommes entrés en contact avec l'ANSSI. Pour nous, c'est un vrai gage de crédibilité qui nous confère le sérieux nécessaire auprès des ministères, des associations et de tous les acteurs du territoire. L'agence intervient à nos côtés sur trois pans : le côté collaboratif, avec l'élaboration de notre architecture IT, à la fois très vaste mais aussi la plus sécurisée possible; la conformité de notre matériel; et enfin, l'aide à la gouvernance du dispositif global. Nous sommes en lien constant et à tous les niveaux : nous travaillons en mode agile. »

DES ÉCHANGES EN BONNE INTELLIGENCE « L'ANSSI est très à l'écoute de nos besoins. Elle sait être conseil, tout en nous laissant l'indépendance de nos actions. ENEDIS se sent responsable vis-à-vis du risque et peut, grâce à l'ANSSI, tout mettre en place pour garantir la défense de son réseau, tout en gardant en vue les objectifs de rentabilité auxquels l'entreprise est soumise. »

En 2016, l'ANSSI a adhéré à l'*Open Information Security Foundation, fondation*, qui pilote notamment le développement de Suricata, logiciel libre largement utilisé dans les solutions de détection d'attaques informatiques. L'enjeu de ce partenariat : concourir à l'émergence de nouveaux moteurs de sondes.

3. CONFORTER LE RAYONNEME

Échanges avec

40

pays

+ de 120

rencontres internationales

6 juillet 2016

Adoption de la directive NIS

NT INTERNATIONAL

L'avènement d'Internet a marqué un tournant dans la perception des notions de frontières et de souveraineté. Le cyber espace nous amène à envisager la géopolitique et la géostratégie avec un regard neuf et une vigilance accrue puisque les menaces s'y multiplient à une vitesse exponentielle. En développant de nombreuses coopérations en Europe et à une échelle plus large, l'ANSSI contribue activement au soutien des positions de la France dans le cyber espace. Son statut interministériel et son approche réglementaire font de l'agence française un modèle de référence qui intéresse un nombre croissant de pays alliés.

DÉVELOPPER L'AUTONOMIE STRATÉGIQUE EUROPÉENNE

Les cyber attaques ne connaissent pas de frontière ! Face à l'évolution du monde numérique et des menaces qui y sont liées, l'Union européenne a pris conscience de la nécessité d'encourager une coopération active entre les États membres autour de la cyber sécurité. Une dynamique multilatérale à laquelle l'ANSSI prend une part majeure.

UN RÔLE CLÉ AU SEIN DE L'EUROPE

La France a été l'un des premiers pays européens à mettre en place une approche ambitieuse en cyber sécurité, notamment via son choix d'utiliser des outils réglementaires pour protéger ses opérateurs d'importance vitale. Ce modèle français interministériel, séparant institutionnellement les rôles d'attaque et de défense, a trouvé un écho auprès d'une majorité d'États membres et des plus hautes autorités européennes sur les questions de sécurité des systèmes d'information. La France joue également un rôle moteur dans la définition des orientations stratégiques de l'Union européenne en matière de cyber sécurité et promeut une vision ambitieuse de la place de l'UE et de ses États membres sur ces questions. Moteur de son action, la France a annoncé officiellement, dans l'objectif 5 de la Stratégie nationale pour la sécurité du numérique, son engagement en faveur de l'autonomie stratégique européenne en matière de sécurité numérique. Cet objectif repose sur trois piliers :

➔ l'autonomie capacitaire, c'est-à-dire le développement de capacité de cyber sécurité à la hauteur des enjeux, au sein de l'Union européenne et de chaque État membre individuellement ;

➔ l'autonomie industrielle et technologique, c'est-à-dire la maîtrise par l'industrie européenne des briques technologiques et des outils industriels essentiels à la sécurité du numérique ;

➔ l'autonomie de décision, c'est-à-dire la préservation de la capacité de l'Union européenne et des États membres à réguler pour faire face aux défis de la sécurité du numérique : protection adéquate des données, préservation de la capacité à évaluer les produits.

Témoin de cet investissement national au sein de l'UE, 2016 a été marquée par deux événements qui ont confirmé le rôle clé aujourd'hui joué par la France dans le paysage européen.

NIS : développer la protection des infrastructures critiques en Europe et la coopération entre États européens

Après près de trois ans de négociation, le Parlement européen et le Conseil de l'Union européenne (UE) ont adopté le 6 juillet 2016 la directive sur la sécurité des réseaux et des systèmes d'information connue sous l'appellation « directive NIS » (pour *Network and Information Security*). L'enjeu : assurer un niveau élevé et commun de sécurité des réseaux et des systèmes d'information dans l'UE. Chef de file en France pour la négociation de ce texte, l'ANSSI se félicite de l'adoption de la directive, qui positionne l'Union européenne en pointe en matière de cyber sécurité.

Concrètement, le texte s'articule autour de quatre axes :
- le renforcement des capacités nationales de cyber sécurité grâce au positionnement de la cyber sécurité comme un enjeu stratégique majeur pour le marché européen du numérique ;
- l'établissement d'un cadre de coopération volontaire entre États membres via un groupe de coopération et un réseau européen des CSIRT *(Computer Security Incident Response Team)* afin de renforcer le cyber résilience ;
- le renforcement par chaque État de la cyber sécurité d'opérateurs de services essentiels ;
- l'instauration de règles européennes communes en matière de cyber sécurité à l'intention des prestataires de services numériques dans le but d'encadrer et de réguler la sécurité du numérique.

Un cPPP qui fait rimer sécurité et compétitivité

Le 5 juillet, la Commission européenne a signé un partenariat public-privé dédié à la cyber sécurité (cPPP). L'enjeu est double puisqu'il s'agit à la fois d'améliorer la cyber résilience de l'Europe et de renforcer la compétitivité des entreprises européennes du secteur de la sécurité numérique. L'objectif de ce nouveau dispositif ? Générer 1,8 milliard d'euros d'investissements via l'effet de levier des 450 millions d'euros provenant des fonds alloués au programme pour la recherche et l'innovation. Réunis au sein de l'*European Cyber Security Organisation* (ECSO, créée en juin 2016), les acteurs du marché de la cyber sécurité devraient, eux, investir trois fois plus. Dans le souci de valoriser les savoir-faire nationaux, l'ANSSI s'est fortement impliquée dans la structuration et l'animation de l'« Équipe France », regroupant l'ensemble des membres français d'ECSO ainsi que les différents ministères concernés par le cPPP. Elle a également engagé un travail de fond pour définir une proposition cohérente sur la certification et la labellisation de sécurité de produits, prestataires et services, qui constituent un axe majeur des travaux engagés par la CE. En octobre, l'ANSSI, représentée par son directeur général Guillaume Poupard, a été élue pour un an à la vice-présidence du conseil d'administration d'ECSO.
Par ailleurs Jean-Baptiste Demaison, chargé d'affaires internationales au sein de l'ANSSI, a été élu président du conseil d'administration de l'Agence européenne pour la sécurité des réseaux et de l'information (ENISA), créée en 2004 pour faciliter la coopération européenne entre États membres autour des questions de sécurité numérique. Pour l'ANSSI, qui accompagne le développement de l'ENISA depuis plusieurs années et prend une part active à ses activités, cette élection est un acte de reconnaissance important qui souligne aussi l'engagement de la France en faveur du renforcement de la cyber sécurité en Europe.

80
missions internationales pour promouvoir et défendre les positions de l'ANSSI

600
pages d'instruction rédigées

110
instructions pour la représentation française à Bruxelles

La transposition de la directive européenne NIS en France, qui sera assurée par l'ANSSI en lien avec l'ensemble des acteurs concernés, bénéficiera des travaux réalisés avec les OIV. La transposition de la directive NIS, entrée en vigueur le 19 juillet 2016, interviendra au plus tard le 9 mai 2018.

Évolutions du contrôle réglementaire

L'année 2016 a par ailleurs pu voir aboutir la réécriture complète de la catégorie 5.2 (contrôlant l'export de certains biens assurant la sécurité de l'information) dans le cadre des travaux de mise à jour de l'arrangement de Wassenaar. Elle devrait être transposée en droit communautaire par un acte délégué d'ici la fin de l'année 2017.

La Commission européenne a émis à la rentrée 2016 sa proposition de révision du règlement européen 428/2009 instituant un régime communautaire de contrôle des exportations de biens à double usage.

En 2016, avec l'inscription de trois nouveaux produits au catalogue du Conseil de l'Union européenne, la France est devenue le premier fournisseur de l'UE en matière de solutions de protection des informations classifiées.

ALLEMAGNE : UNE COOPÉRATION BILATÉRALE DYNAMIQUE

Depuis de nombreuses années, l'ANSSI et son homologue allemand, le *Bundesamt für Sicherheit in der Informationstechnik* (BSI) coopèrent au renforcement de la sécurité du numérique dans leurs pays respectifs mais aussi dans tout l'espace européen. En 2016, la dynamique partenariale s'est encore accentuée à travers plusieurs actions: implication commune dans le cPPP, participation conjointe au forum international de la Cyber Sécurité de Lille (janvier), au salon ItSa de Nuremberg (octobre), etc. Ensemble, les deux agences ont également fortement contribué à la rédaction des spécifications techniques encadrant les produits et services conformes au règlement eIDAS. Entré en application en juillet, ce règlement permet une reconnaissance uniforme des moyens d'identification et d'authentification électronique (dont la signature électronique) au sein de l'Union européenne. Et pour clôturer cette nouvelle année de coopération, le lancement en décembre d'un label commun franco-allemand ESCloud *(European Secure Cloud)* destiné aux prestataires de services d'informatique en nuage *(cloud computing)* a apporté une belle illustration de la vision partagée de l'Allemagne et de la France en matière de sécurité du numérique.

Paroles d'acteurs

Bundesamt für Sicherheit in der Informationstechnik

Arne Schönbohm,

président du BSI

ANSSI-BSI : DES RELATIONS PRIVILÉGIÉES « L'ANSSI et le BSI entretiennent de longue date des relations basées sur la confiance et la reconnaissance mutuelle. Les agences travaillent en étroite coopération sur les volets de la prévention, de la détection et de la réaction aux incidents afin d'assurer et de renforcer la cyber sécurité dans les deux pays. »

FRANCE ET ALLEMAGNE FACE À UNE MENACE CYBER « Pour contrer la menace, l'ANSSI et le BSI ont chacun une bonne compréhension des enjeux liés à la cyber sécurité au sein des deux pays mais aussi au niveau européen. Les approches françaises et allemandes sont similaires et complémentaires afin de permettre à l'ANSSI et au BSI de bénéficier d'un fructueux partage d'expériences, de concepts et d'idées. »

LE PARTAGE D'INFORMATIONS : UN PILIER ESSENTIEL DE LA CYBER SÉCURITÉ « En échangeant rapidement des informations opérationnelles, l'ANSSI et le BSI peuvent faire face à des menaces cyber dans leur pays respectif immédiatement et contrer des attaques. La coopération et le partage d'informations entre l'ANSSI et le BSI contribuent également à une meilleure compréhension de l'état de la menace cyber, ce qui bénéficie *in fine* à l'ensemble des acteurs, français et allemands, de la cyber sécurité, notamment les industriels, les infrastructures critiques et les citoyens. »

LES CHALLENGES À VENIR « En 2017, l'un des principaux sujets de coopération et de partage d'information concerne les enjeux de la sécurité informatique des élections en France et en Allemagne. Sur le volet de la prévention, l'ANSSI et le BSI travaillent en étroite collaboration pour élaborer des standards et des projets communs. Le label ESCloud, qui s'attache à la sécurité des solutions d'informatique en nuage (le *cloud),* est un exemple récent d'un projet de coopération mené avec succès par l'ANSSI et le BSI. Le BSI espère continuer et renforcer ce partenariat d'exception. »

SecNumCloud : les fruits de la collaboration franco-allemande

En 2014, l'ANSSI avait publié un premier référentiel destiné aux prestataires de services cloud. En décembre 2016, une nouvelle version baptisée SecNumCloud a été rendue publique à la suite d'une expérimentation menée avec quatre acteurs (*Orange Cloud for Business*, Intrinsec, Oodrive et Vendôme Solution). Au lendemain de ce lancement, l'ANSSI et le BSI ont présenté ensemble un label franco-allemand appuyé à la fois sur SecNumCloud et sur le catalogue allemand C5. Nommé ESCloud pour *European Secure Cloud*, ce « socle de confiance » se compose de 15 règles techniques et organisationnelles élaborées sur la base de l'expérience de la France et de l'Allemagne en matière de certification et de qualification de produits et de services de sécurité. Réservé pour l'heure aux schémas de qualification de prestataires qualifiés par les deux États, ce label devrait être à terme étendu à d'autres partenaires européens.

L'ANSSI a poursuivi son implication en lien direct avec le SGDSN dans le programme européen de radio navigation Galileo, ce système de positionnement par satellites développés par l'UE dont le déploiement doit s'achever courant 2020. Son avancée se traduit tant en ce qui concerne la validation des produits de sécurité et protocoles cryptographiques du dispositif que pour la sécurisation des éléments secrets (clés cryptographiques) embarqués dans les satellites eux-mêmes. Galileo est pour l'Europe un bon moyen d'assurer son autonomie, sa souveraineté en matière de géolocalisation.

Conclusions du Conseil franco-allemand de défense et de sécurité (CFADS) de 2016 :

➔ La France et l'Allemagne partagent le même objectif d'une autonomie stratégique européenne numérique, fondée sur : le renforcement de la capacité des États membres et de l'UE à protéger leurs réseaux et à renforcer leur résilience numérique, en appelant conjointement à une mise en œuvre dès que possible de la directive NIS - Network and Information Security ; le développement d'une industrie européenne autonome, innovatrice, efficace et diversifiée, en particulier dans le domaine du numérique de confiance et de la cybersécurité ; la garantie d'une capacité des Européens à décider de manière autonome du niveau de sécurité de leurs données, notamment dans le contexte de négociation de traités commerciaux.
La France et l'Allemagne ont pris plusieurs initiatives dans ce domaine, à l'instar de leurs efforts communs entrepris dans le domaine de la certification de sécurité du *cloud computing* ou de la sécurité des e-mails, de l'organisation d'un *speed dating* entre PME de cybersécurité françaises et allemandes en marge du Forum international de la cybersécurité à Lille en janvier 2016, ou dans le cadre de leur action diplomatique commune sur la sécurité internationale du cyberespace, notamment à l'ONU, à l'OSCE, à l'UE et à l'OTAN.

PROMOUVOIR LE MODÈLE FRANÇAIS À L'INTERNATIONAL

Enjeux économiques, stratégiques, politiques… La sécurité du numérique confronte plusieurs modèles et visions du cyber espace. Au-delà des limites européennes, le modèle français s'exporte et constitue aujourd'hui une référence internationale.

À l'heure où la cyber menace se globalise, la coopération à l'échelle mondiale s'impose plus que jamais comme une nécessité. L'ANSSI fait des relations internationales l'un des fers de lance de son action. Dans cette optique, elle a noué en 2016 des relations avec une quarantaine de pays, adaptant ses coopérations au niveau de maturité cyber de ses interlocuteurs. Aujourd'hui, un de ses axes d'action consiste à mettre en place des relations bilatérales avec un grand nombre d'agences homologues sur tous les continents, coordonnées par le bureau des Relations internationales. En 2016, l'ANSSI a poursuivi le développement de son réseau de partenaires au-delà de l'espace européen, notamment à travers le rapprochement avec le Japon, Singapour et l'Australie, acteurs majeurs de la cyber sécurité en Asie et en Océanie, mais également avec de nombreux pays d'Afrique.

Un ambassadeur des positions hexagonales…

L'ANSSI participe aussi à la défense de la position française concernant les enjeux politiques relatifs à la cyber sécurité. À ce titre, elle contribue de manière importante aux travaux du groupe d'experts gouvernementaux de l'ONU. En 2016, l'agence a en particulier formulé plusieurs propositions de normes de comportements prenant appui sur l'expertise acquise en matière de défense des infrastructures critiques.

… au service de la protection du cyber espace planétaire

L'ANSSI s'attache également à partager ses savoir-faire avec d'autres acteurs, organisations internationales ou autorités nationales. Très présente auprès de l'Union européenne et de l'Otan – où elle préside des groupes de travail sur les communications voix sécurisées et le chiffrement IP –, l'agence a poursuivi son action auprès de l'Organisation des Nations unies (ONU) et de l'Agence spatiale européenne (ESA). Elle a par ailleurs développé ses activités de soutien au développement capacitaire à travers plusieurs coopérations bilatérales, notamment avec le Maroc (2015) le Sénégal et Monaco (2016), et un soutien continu à l'initiative AfricaCERT, qui se veut une plateforme d'échange entre CSIRT africains.

Un CERT *(Computer Emergency Response Team)* ou CSIRT *(Computer Security Incident Response Team)* est une structure chargée de réagir en cas d'incident informatique. L'ANSSI opère le CERT-FR, dont le périmètre couvre l'administration française et les OIV.

DE LA STRATÉGIE À **L'OPÉRATIONNEL**

Alicia

« Lorsque j'ai intégré la sous-direction Relations extérieures et Coordination (RELEC) de l'ANSSI à l'issue d'un master en sciences politiques, le bureau des Relations internationales (RIT) ne comptait que deux autres agents. Et avec mon profil orienté sciences humaines, j'étais pour le moins atypique dans le paysage très scientifique de l'agence ! Mais, depuis, les choses ont considérablement changé : le bureau RIT compte actuellement une quinzaine d'agents et je croise de plus en plus de personnes avec un parcours proche du mien. Moi-même, j'ai évolué : en mars 2016, j'ai bénéficié d'une mobilité interne pour rejoindre le Centre opérationnel (COSSI) de l'ANSSI en tant que responsable des relations opérationnelles avec les partenaires étrangers. Ma mission comporte un volet préparation opérationnelle, avec notamment une participation aux exercices et aux rencontres entre CSIRT ou au sein des communautés européennes et internationales (EGC*, réseau européen des CSIRT, ou encore FIRST**…).
Un second appui opérationnel vise la coordination des échanges avec nos partenaires afin de mieux saisir l'état de la menace et pouvoir faire face de manière coordonnée aux situations de crise. Même si j'ai changé de sous-direction, mon rôle actuel s'inscrit dans le prolongement de l'action du bureau RIT et mon arrivée au COSSI illustre la volonté de l'agence d'enrichir et de développer son positionnement à l'international. »

* EGC: *European Goverment CERT*, qui regroupe une douzaine de CSIRT gouvernementaux européens échangeant sur les menaces et les incidents visant les principaux secteurs d'activité des États.

** FIRST: *Forum of Incident Response and Security Team*. Regroupant près de 300 CSIRT et CERT, ce cercle de confiance permet d'échanger les bonnes pratiques et l'information récoltée par les différentes équipes travaillant sur le sujet cyber sécurité au niveau mondial.

Destiné à accroître la visibilité des solutions françaises de sécurité numérique à l'international, le label France Cybersecurity poursuit son développement avec l'inscription de 41 nouvelles offres au catalogue.

Soutien à l'export

Les sollicitations pour associer des entreprises françaises à des événements internationaux sont nombreuses et croissantes depuis 2015. Elles émanent de partenaires étrangers, d'autorités françaises ou d'acteurs privés du développement économique tels que Business France ou CEIS concernant des événements dédiés à la cyber sécurité.

Le modèle national de cyber sécurité s'appuyant sur le développement d'un secteur privé national dynamique, l'ANSSI associe systématiquement la présentation du secteur privé et de la politique industrielle française (notamment l'approche de qualification de prestataires) à ses actions de valorisation du modèle national. En complément, l'agence est toujours disposée à mettre en relation les pays ou organisations internationales qui en font la demande avec des entreprises françaises du secteur.

L'ANSSI développe également son action dans les salons en assurant une présence « France » fédérée, en encourageant la participation d'entreprises et de l'agence, dans certains cas sur un même pavillon France.

Des actions complémentaires sont également mises en place au cas par cas : rencontres entre entreprises et représentants français en poste sur le marché local, pour développer des relais locaux pour les entreprises, rencontres entre entreprises françaises et clients ou partenaires locaux potentiels, le cas échéant en relayant l'action à Business France, fourniture des informations utiles aux entreprises sur l'accès au marché visé.

BIBLIOGRAPHIE

DOCUMENTS DE DOCTRINE

Documents mis à jour

• Note technique DAT-NT-04/ANSSI/SDE/NP *Recommandations de sécurité relatives à la télé-assistance*, 13 janvier 2017

• Note technique DAT-NT-008/ANSSI/SDE/NP *Recommandations de sécurité relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows*, 18 juillet 2016

• Note technique DAT-NT-13/ANSSI/SDE/NP *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows*, 13 janvier 2017

• Note technique DAT-NT-27/ANSSI/SDE/NP *Déploiement et configuration centralisés d'EMET pour le durcissement des postes de travail et des serveurs Microsoft Windows*, 26 octobre 2016

Nouveaux documents

• Note technique DAT-NT-28/ANSSI/SDE/NP *Recommandations de configuration d'un système GNU/Linux*, 12 janvier 2016

• Note technique DAT-NT-25/ANSSI/SDE/NP *Recommandations pour la sécurisation d'un commutateur de desserte*, 24 juin 2016

• Note technique DAT-NT-29/ANSSI/SDE/NP *Recommandations pour une utilisation sécurisée de Zed!*, 12 janvier 2016

• Note technique DAT-NT-31/ANSSI/SDE/NP *Recommandations de sécurisation d'un pare-feu SNS*, Version 1.2, 21 avril 2016

• Note technique DAT-NT-32/ANSSI/SDE/NP *Recommandations et méthodologie pour le nettoyage d'une politique de filtrage réseau d'un pare-feu*, 4 août 2016

• Note technique DAT-NT-34/ANSSI/SDE/NP *Recommandations de sécurité pour les architectures basées sur Vmware vSphere ESXi*, 25 mai 2016

• Guide SDE-NT-35/ANSSI/SDE/NP *Recommandations de sécurité relatives à TLS*, juillet 2016

• Note technique DAT-NT-36/ANSSI/SDE/NP *Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10*, 20 janvier 2017

• *La cybersécurité des systèmes industriels : cas pratique d'un tunnel routier*, Parties 1 et 2, octobre 2016

• *Guide d'hygiène informatique – Renforcer la sécurité de son système d'information en 42 mesures*, Version 1.0, janvier 2017

• *Guide des bonnes pratiques de sécurité informatique à bord des navires*, Version 1.0, octobre 2016

• *Best Practices for Cyber Security On-board Ships*, Version 1.0, octobre 2016

Référentiels

• *Exigences de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels*, mars 2016

• *Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage*, décembre 2016

Bulletins d'information

• *Bulletin hebdomadaire d'actualité du CERT-FR : cert.ssi.gouv.fr/site/index_act.html*

• *Note d'information du CERT-FR relative aux systèmes obsolètes : cert.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html*

PUBLICATIONS SCIENTIFIQUES

• Jean-Sébastien Coron, Thomas Holenstein, Robin Künzler, Jacques Patarin, Yannick Seurin, Stefano Tessaro : *How to Build an Ideal Cipher : The Indifferentiability of the Feistel Construction*, Journal of Cryptology, vol. 29, pp. 61-114, Springer 2016

• Aurélie Bauer, Eliane Jaulmes, Emmanuel Prouff, Jean-René Reinhard, Justine Wild : *Horizontal collision correlation attack on elliptic curves – Extended Version*, Cryptography and Communications, vol. 7, pp. 91-119

• Thomas Peyrin, Yannick Seurin : *Counter-in-Tweak : Authenticated Encryption Modes for Tweakable Block Ciphers*, CRYPTO 2016, LNCS 9816, pp. 33-63, Springer 2016

• Benoît Cogliati, Yannick Seurin : *An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC*, CRYPTO 2016, LNCS, pp. 121-149, Springer 2016

• Jérémy Jean, Ivica Nikolic : *Efficient Design Strategies Based on the AES Round Function*, FSE 2016, LNCS 9783, pp. 334-353, Springer 2016

• Benoît Cogliati, Yannick Seurin : *Strengthening the Known-Key Security Notion for Block Ciphers*, FSE 2016, LNCS, pp. 494-513, Springer 2016

• Jean-Pierre Flori : *A conjecture about Gauss sums and bentness of binomial Boolean functions*. arXiv : 1608.05008 (2016), presented at WAIFI 2016

• Luca De Feo, Cyril Hugounenq, Jérôme Plût, Éric Schost : *Explicit isogenies in quadratic time*, ANTS 2016, London Mathematical Society 2016

• P. Chifflier : *Securing Security Tools*, SuriCon 2016

• Arnaud Ebalard, Arnaud Fontaine, David Diallo, Jean-Pierre Flori, Karim Khalfallah, Mathieu Renard et Ryad Benadjila : *Eurisko : développement d'une carte électronique*, SSTIC 2016

• Guillaume Bouffard et Julien Lancia : *Fuzzing and overflows in Java Card Smart Cards*, SSTIC 2016

• Sonia Belaïd, Fabrice Benhamouda, Alain Passelègue, Emmanuel Prouff, Adrian Thillard, Damien Vergnaud : *Randomness Complexity of Private Circuits for Multiplication*, EUROCRYPT 2016

• Fabrice Benhamouda, Céline Chevalier, Adrian Thillard, Damien Vergnaud: *Easing Coppersmith Methods Using Analytic Combinatorics : Applications to Public-Key Cryptography with Weak Pseudorandomness*, PKC 2016

• Patrick Haddad, Chaouki Kasmi, José Lopes Esteves et Valentin Houchouas : *Electromagnetic Harmonic Attack on Transient Effect Ring Oscillator Based True Random Number Generator*, HARDWEAR.IO 2016

• Christoph Dobraunig, Maria Eichlseder, Thomas Korak, Victor Lomné, Florian Mendel: *Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes*, ASIACRYPT 2016

• Florent Bruguier, Pascal Benoit, Lionel Torres, Lyonel Barthe, Morgan Bourree, Victor Lomné : *Cost-Effective Design Strategies for Securing Embedded Processors*, IEEE Transactions on Emerging Topics in Computing

• Noreddine El Janati El Idrissi, Guillaume Bouffard, Jean-Louis Lanet et Said El Hajji *: Trust can be misplaced*, Journal of Cryptographic -Engineering

• P.-M. Ricordel, E. Alincourt, C. Ray, D. Daré-Emzivat, A. Boudraa : *Methodology for AIS Signature Identification through Magnitude and Temporal Charaterization*, OCEANS 2016 MTS/IEEE, Shanghai, Chine

• P.-M. Ricordel, E. Alincourt, C. Ray, D. Daré-Emzivat, A. Boudraa : *Méthodologie d'extraction de signatures issues des signaux AIS*, SSTIC 2016, Rennes, France

• B. Michau, C. Devine: *How not to break LTE crypto*, SSTIC 2016, Rennes, France

• C. Kasmi, S. Lalléchère, J. Lopes Esteves, P. Bonnet, S. Girard, F. Paladian, E. Prouff : *Re-sampling techniques for EMC/EMI testing: motivations and validations throughout experiments*. IEEE Transactions on EMC 2016

• C. Kasmi, J. Lopes Esteves : *Functional Susceptibility of COTS devices to IEMI at local and large-scale levels*, ICEAA 2016, Cairns, Australia, 09/2016

• C. Kasmi, S. Lalléchère, J. Lopes Esteves, S. Girard, P. Bonnet, F. Paladian : *Re-sampling optimized technique applied to EMC TL issues*, EUROEM 2016, Londres, UK, 08/2016

• C. Kasmi, J. Lopes Esteves, P. Valembois : *Susceptibility testing for detecting IEMI-based covert channels*, EUROEM 2016, Londres, UK, 08/2016

• S. Lalléchère, C. Kasmi, J. Lopes Esteves, S. Girard, P. Bonnet, F. Paladian : *Apport de l'analyse statistique de ré-échantillonnage pour l'optimisation CEM*, CEM 2016, Rennes, France, 08/2016

• V. Houchouas, C. Kasmi, J. Lopes Esteves: *Étude comportementale d'un logiciel lors d'agressions EM pour la SSI*, CEM 2016, Rennes, France, 08/2016

• C. Kasmi, S. Lalléchère, L. Patier, J. Lopes Esteves, S. Girard, P. Bonnet, F. Paladian : *Optimization of EMC Aerospace Margins using Re-Sampling Techniques with Monte Carlo Simulations*, MetroAeroSpace Conference 2016, Italy, 06/2016

• C. Kasmi, J. Lopes Esteves : *Whisper in the Wire: Voice Command Injection Reloaded*, Hack In Paris 2016, Paris, France, 06/2016

• C. Kasmi, J. Lopes Esteves, Keith Armstrong: *EMC/EMI and Functional Safety: Methodology to characterize effects of interferences on devices*, Asia Pacific International Symposium on EMC 2016, Shenzen, China, 05/2016

• Mickaël Salaün : *Landlock LSM: Unprivileged sandboxing*, Kernel Recipes 2016

• Thomas Letan, Pierre Chifflier, Guillaume Hiet, Pierre Néron, Benjamin Morin: *SpecCert: Towards Verified Hardware-based Security Enforcement*, FM 2016

• Mathieu Renard, Ryad Benadjila : *Security Offense and Defense Strategies: video-game consoles architecture under microscope*, Hack in Paris 2016

• Mickaël Salaün, Marion Daubignard, Hervé Debar : *Stemjail: Dynamic Code Compartmentalization*, AsiaCCS 2016

• Arnaud Ébalard, Ryad Benadjila, Mathieu Renard, Arnaud Fontaine : *Projet Eurisko*, SSTIC 2016

• Yves-Alexis Perez : *Noyaux Linux durcis*, SSTIC 2016

• Florian Maury, Mickaël Bergem : *A first glance at the U2F protocol*, SSTIC 2016

• Adrien Chevalier, Stéfan Le Berre, Tristan Pourcelot : *Démarche d'analyse collaborative de codes malveillants*, SSTIC 2016

• Pierre Capillon : *Cryptanalyse en boîte noire de chiffrement propriétaire: étude de cas*, SSTIC 2016

• Aurélien Bordes : *Windows Error Reporting*, SSTIC 2016

Articles acceptés en 2016 à paraître en 2017

• Colin Chaigneau and Henri Gilbert : *Is AEZ v4.1 Sufficiently Resilient Against Key-Recovery Attacks*, to appear in IACR Transactions in Symmetric Cryptology, FSE 2017

• Jian Guo, Jérémy Jean, Ivica Nikolic, Kexin Qiao, Yu Sasaki and Siang Meng Sim : *Invariant Subspace Attack Against Midori64 and the Resistance Criteria for S-box Designs*, to appear in IACR Transactions in Symmetric Cryptology, FSE 2017

• Jian Guo, Jérémy Jean, Ivica Nikolic and Yu Sasaki : *Meet-in-the-Middle Attacks on Classes of Contracting and Expanding Feistel Constructions*, to appear in IACR Transactions in Symmetric Cryptology, FSE 2017

• Jérémy Jean : *Cryptanalysis of Haraka*, to appear in IACR Transactions in Symmetric Cryptology, FSE 2017

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
@ANSSI_fr