RAPPORT ANNUEL

2012

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*
Gestion de projet : *Anne-Catherine Belliot, Séverine Oger*
Coordination éditoriale et rédaction : *Anne-Catherine Belliot*
Coordination graphique : *Marc Renaudin*
Conception et réalisation : *Chien Jaune studio | chienjaunestudio.com*
Secrétariat de rédaction : *Prop'OSE communication | prop-ose.fr*
Crédits photos : *Patrick Gaillardin / Fix / ANSSI*
Illustrations : *Chien Jaune studio*
Remerciements à nos partenaires ainsi qu'à l'ensemble des agents de l'ANSSI pour leurs témoignages et leur participation à l'élaboration de ce rapport.

SOMMAIRE

CLAIRE LANDAIS

SECRÉTAIRE GÉNÉRALE DE LA DÉFENSE
ET DE LA SÉCURITÉ NATIONALE

GUILLAUME POUPARD

DIRECTEUR GÉNÉRAL DE L'ANSSI

EN QUOI 2018 FUT-ELLE UNE ANNÉE PARTICULIÈRE POUR L'ANSSI ?

Claire Landais
À mon arrivée au SGDSN, j'ai été frappée par la capacité de l'ANSSI à assurer à la fois la sensibilisation et l'accompagnement dans la cybersécurité d'une part, et la conduite des opérations de cyberdéfense d'autre part, avec cohérence et réactivité. Un an plus tard et cette première impression confirmée, je constate à quel point cette polyvalence fait de l'agence une entité reconnue et estimée de ses interlocuteurs. Voilà qui explique comment elle parvient à fédérer ses partenaires autour d'elle.

Guillaume Poupard
Le constat est sans appel : 2018 prouve une nouvelle fois que le risque numérique, loin d'être éthéré, doit être au cœur de nos préoccupations. Et pas seulement celles de l'ANSSI ! Les attaques informatiques touchent toute la société. C'est pourquoi nous devons tous nous emparer du sujet. Cette conviction, je la partage avec de nombreux acteurs et l'année 2018 nous a donné l'occasion de l'exprimer collectivement. L'Appel de Paris, le Cybersecurity Act, les accords de coopération sectoriels ou encore la participation de l'agence à la communauté Open Source en sont de parfaits exemples.

L'ANSSI N'A DE CESSE DE RAPPELER L'IMPORTANCE D'UNE RESPONSABILITÉ PARTAGÉE VIS-À-VIS DU RISQUE NUMÉRIQUE. OÙ EN SOMMES-NOUS ?

Claire Landais
La crédibilité dont jouit l'ANSSI auprès des décideurs publics permet une mobilisation face aux risques numériques. Mais bien que la prise de conscience progresse et que le cadre législatif et réglementaire s'améliore régulièrement, changer de regard sur la cybersécurité prend du temps. De plus, la prise de conscience ne peut pas être strictement nationale. Elle doit tenir compte de réflexions communes menées à l'échelle européenne. Nous avons encore beaucoup de travail devant nous.

Guillaume Poupard
Je commencerai par faire deux constats. D'abord, les attaquants exploitent de plus en plus les relations de confiance établies entre partenaires pour accéder aux informations qu'ils convoitent. Ensuite – et c'est encore plus inquiétant –, des groupes très organisés s'emploient à préparer ce qui ressemble aux conflits de demain en s'introduisant dans les infrastructures des systèmes les plus critiques. La « bonne nouvelle » dans tout ça, c'est qu'il devient de plus en plus difficile pour les décideurs d'ignorer cette menace. Progressivement, on assiste au sein des organisations à un rapprochement entre sécurité numérique et préoccupations économiques, politiques et sociétales.

QUELS SONT VOS SOUHAITS POUR L'ANSSI À L'OCCASION DE SES 10 ANS ?

Claire Landais
Au SGDSN se côtoient une diversité de statuts, de cultures et de profils que le sens du service public et les missions au profit du plus haut niveau de l'État rassemblent. C'est ce qui fait la richesse de cette maison. L'une de nos missions historiques est d'identifier les champs d'action qui nous mobiliseront demain. En 2019, comme en 2009, au bout de dix années incroyablement riches et parfois dramatiques, ce souci de l'avenir et cette volonté d'anticiper les menaces qui pourraient frapper notre pays et nos concitoyens rassemblent le SGDSN et l'ANSSI plus que jamais.

Guillaume Poupard
Je souhaite que l'ANSSI continue de s'ouvrir et de rassembler autour d'elle avec l'enthousiasme qui la caractérise et que j'espère communicatif. Car la cybersécurité constitue en elle-même un champ d'innovation passionnant, profondément transdisciplinaire, riche d'une grande diversité de profils et qui, trop lentement, attire de plus en plus de femmes. Enfin, je dirais que 10 ans, c'est l'occasion de prendre du recul sur le chemin parcouru. Mais c'est aussi et surtout l'occasion pour moi de rappeler le plaisir que j'ai à travailler aux côtés d'agents animés par tant d'exigence et de passion.

ANALYSE DE LA MENACE en 2018

5 GRANDES TENDANCES OBSERVÉES EN FRANCE ET EN EUROPE

L'analyse de la menace offre un aperçu des tendances observées par la sous-direction opérations de l'ANSSI au cours de l'année 2018. Malgré la difficulté de représenter le cyberespace, la menace doit être contextualisée. Les tendances qui suivent sont donc décrites au regard des objectifs visés par l'attaquant et des modes opératoires employés par celui-ci pour atteindre son objectif.

EXFILTRATION DE DONNÉES STRATÉGIQUES

La compromission de systèmes d'information à des fins d'espionnage n'est pas un fait nouveau et ces attaques ont représenté en 2018 une préoccupation majeure pour l'ANSSI. **Un intérêt renforcé des attaquants à l'égard de secteurs d'activité d'importance vitale et infrastructures critiques spécifiques a pu être constaté**, à l'instar des secteurs de la défense, de la santé ou encore de la recherche.

Cette menace se caractérise par l'extrême discrétion dont font preuve les groupes d'attaquants et le soin apporté à la phase de planification. Leurs modes opératoires s'appuient généralement sur un haut degré de sophistication technique et leurs attaques – très ciblées – s'étalent sur de longues périodes. D'importants moyens logistiques, humains et financiers sont mobilisés par les attaquants pour atteindre de tels objectifs.

ATTAQUES INDIRECTES

De plus en plus d'attaquants choisissent de compromettre une cible intermédiaire (fournisseur, prestataire, etc.) et d'exploiter la relation de confiance qui l'unit à la cible finale pour toucher cette dernière. **La menace que représentent les attaques indirectes augmente au fur et à mesure que les cibles finales se sécurisent.**

Les attaquants parviennent ainsi à contourner les mesures de sécurité de très grandes organisations qui sont de plus en plus conscientes du risque numérique et de la nécessité de s'en prémunir. La compromission d'un seul intermédiaire suffit parfois à obtenir un accès privilégié à plusieurs organisations, démultipliant ainsi le retour sur investissement pour les attaquants. Ils peuvent alors mener des campagnes d'ampleur visant de multiples cibles à fort intérêt stratégique.

OPÉRATIONS DE DÉSTABILISATION OU D'INFLUENCE

Les attaques informatiques menées à des fins de déstabilisation ou d'influence ont été particulièrement nombreuses en 2018. Ces incidents sont généralement le fait de groupes d'individus et peuvent prendre de multiples formes.

Ces attaques présentent toutefois quelques points communs : un degré de technicité modéré, des cibles choisies pour leur apparente vulnérabilité et des conséquences pouvant aller de la simple indisponibilité du service impacté au véritable sabotage. Fait notable, ces attaques peuvent être revendiquées depuis la France ou l'étranger par des individus isolés comme par des groupes d'attaquants.

GÉNÉRATION DE CRYPTOMONNAIES

Tout au long de l'année 2018, l'ANSSI a pu observer une multiplicité d'attaques ayant pour finalité l'enrichissement des attaquants. En particulier, ils profitent des failles de sécurité de ces systèmes d'information pour compromettre un grand nombre d'équipements par le dépôt discret de mineurs de cryptomonnaies. Ils peuvent alors se servir de la puissance de calcul cumulée de ces systèmes pour générer de la cryptomonnaie.

Contrairement aux rançongiciels, ces logiciels malveillants se font les plus discrets possibles. L'année 2018 a mis en évidence une tendance qui pousse ces cybercriminels à s'organiser en réseaux.

FRAUDE EN LIGNE

Les tentatives de fraude en ligne représentent une menace permanente sur Internet. Toutefois, à travers les incidents que l'ANSSI a dû traiter, un certain nombre d'évolutions récentes liées aux cibles, aux objectifs et à l'ampleur de cette menace ont pu être observées.

La préoccupation croissante des opérateurs à l'égard des enjeux de sécurité numérique et le renforcement parallèle de leurs capacités de défense amènent nombre d'attaquants à se tourner vers des cibles moins exposées mais plus vulnérables. Ainsi, de nombreuses campagnes d'hameçonnage ciblant des collectivités territoriales ou des acteurs du secteur de la santé ont été observées en 2018. Les objectifs de ces campagnes sont multiples mais comprennent généralement le vol de données personnelles, la demande de paiement d'une rançon après chiffrement des données, le minage de cryptomonnaies et la constitution de réseaux de machines zombies (*botnets*).

Cette analyse ne saurait être considérée comme une représentation exhaustive de l'actualité opérationnelle de l'ANSSI.

ACTUALITE OPÉRATIONNELLE*

1 869
signalements

–

391
incidents hors opérateurs d'importance vitale (OIV)

–

16
incidents majeurs

–

14
opérations de cyberdéfense

* *Nombre d'interventions menées par l'ANSSI en 2018*

L'analyse de la menace reflète l'actualité opérationnelle de l'ANSSI. Si les attaques les plus visibles prennent la forme d'opérations de sabotage, l'espionnage est sans nul doute le risque qui pèse le plus fortement sur les organisations. En 2018, l'agence s'est montrée particulièrement attentive aux évolutions que connait cette menace.

// PRAGMATISME ET RESPONSABILITÉ PARTAGÉE

Nous évoluons au sein d'écosystèmes complexes, mouvants et de plus en plus interconnectés. Les menaces suivent une dynamique analogue, faisant de la sécurité numérique un véritable enjeu. Il est urgent de diffuser à tous les niveaux une culture de la sécurité numérique.

COMPRENDRE POUR DÉCIDER

L'analyse de risque est au cœur du management du risque numérique. Pour accompagner la transformation numérique et ses acteurs vers plus de sécurité, l'ANSSI s'est engagée, aux côtés d'autres partenaires, dans une démarche de modernisation de la méthode d'analyse de risques EBIOS. Innovante et pratique, la méthode rebaptisée EBIOS Risk Manager s'adapte aux nouveaux enjeux de sécurité numérique.

Elle permet de dépasser la seule approche technique pour encourager la création et la mise en œuvre de politiques de management des risques numériques complètes, adaptées et intégrées au plus haut niveau décisionnel.

« Les attaques WannaCry et NotPetya sont passées par là. Il est temps de considérer le risque numérique comme un risque à part entière pour l'entreprise. »

Guillaume Poupard,
directeur général de l'ANSSI

L'ensemble des parties prenantes doit prendre part à cet effort d'anticipation. Il doit permettre aux décideurs de prendre des décisions éclairées, génératrices de résultats durables.

Une démarche collaborative et agile

EBIOS Risk Manager est une méthode conçue pour être éprouvée, discutée et améliorée au sein d'une large communauté d'utilisateurs. Si le club EBIOS et le Club de la sécurité de l'information français (CLUSIF), partenaires historiques de la démarche, sont garants de la reconnaissance et de l'utilisation de la méthode, il est essentiel d'associer d'autres organismes professionnels pour la faire évoluer au contact de la réalité des organisations.

Un label pour outiller la méthode

La labellisation EBIOS Risk Manager s'adresse aux éditeurs de logiciels désireux de développer des outils conformes à la méthode. L'objectif est de faciliter la démarche des utilisateurs et de parvenir à une meilleure appropriation des concepts permettant de mener l'analyse de risque à son terme.

2017

2018

UNE PRÉSENCE RENFORCÉE

2018 fut pour l'ANSSI une année de mutation, moins marquée par son intensité opérationnelle que par le renforcement de son positionnement. En faisant évoluer son organisation interne et en l'éprouvant, l'agence adapte avec cohérence les contours de son champ d'action. En défendant la position française sur les thèmes qui mobilisent la communauté européenne et internationale, elle fait valoir son expérience et son expertise.
Enfin, en prenant un temps d'avance sur les tendances, elle entraîne avec elle une large communauté d'acteurs qui, plus que jamais, doivent s'approprier les enjeux de sécurité numérique.

16 ET 17 JANVIER
MÉTRO PIRATE 17 ET SECNUM 17

24 JANVIER
LE MOOC SECNUMACADÉMIE RÉCOMPENSÉ DE DEUX PRIX

30 JANVIER
CYBER SOPEX 18

7 FÉVRIER
L'ANSSI LANCE UNE CAMPAGNE DE SENSIBILISATION POUR LES JEUX OLYMPIQUES D'HIVER

26 FÉVRIER
PROMULGATION DE LA LOI N°2018-133 DE TRANSPOSITION DE LA DIRECTIVE EUROPÉENNE NETWORK AND INFORMATION SECURITY (NIS)

26 MARS
INTERVENTION DE L'ANSSI À LA GLOBAL ENCRYPTION CONTROL CONFERENCE *(SAN FRANCISCO)*

24 AU 27 AVRIL
LA FRANCE REMPORTE LA 1E PLACE AU CLASSEMENT DE L'EXERCICE DE CYBERDÉFENSE ORGANISÉ PAR L'OTAN

22 ET 23 MAI
VIGIPIRATE 18

25 MAI
PUBLICATION DU DÉCRET D'APPLICATION POUR LA DIRECTIVE NIS

RGPD
28 MAI

6 ET 7 JUIN
CYBER EUROPE 18

13 JUIN *COUPE DU MONDE 2018*
L'ANSSI LANCE UNE CAMPAGNE DE SENSIBILISATION POUR LA COUPE DU MONDE DE FOOTBALL

14 JUIN
L'ANSSI REMET SES PREMIERS VISAS DE SÉCURITÉ

13 JUILLET
PROMULGATION DE LA LOI DE PROGRAMMATION MILITAIRE (LPM) 2019-2025

6 AOÛT
LANCEMENT ET MISE EN SERVICE DE QUATRE SATELLITES GALILEO DONT LA SÉCURITÉ REPOSE EN PARTIE SUR DES CLÉS GÉNÉRÉES PAR L'ANSSI

19 SEPTEMBRE
OUVERTURE DU CODE SOURCE DE CLIP OS, LE SYSTÈME D'EXPLOITATION DURCI CONÇU PAR L'ANSSI

28 SEPTEMBRE
PUBLICATION DE L'ARRÊTÉ DU 14/09 FIXANT LES RÈGLES DE SÉCURITÉ S'APPLIQUANT AUX OPÉRATEURS DE SERVICES ESSENTIELS (OSE)

OCTOBRE
MOIS EUROPÉEN DE LA CYBERSÉCURITÉ

9 OCTOBRE
EXERCICE GROUPE DE PLACE ROBUSTESSE

10 AU 13 OCTOBRE
LANCEMENT DE LA MÉTHODE D'ANALYSE DE RISQUE EBIOS RISK MANAGER

14 AU 17 OCTOBRE
L'ÉQUIPE FRANCE REMPORTE LA 2E PLACE DU CHALLENGE EUROPÉEN ORGANISÉ À LONDRES FACE À 16 AUTRES ÉQUIPES

6 AU 15 NOVEMBRE
HAND SPINNER
LA SOUS-DIRECTION OPÉRATIONS MET SA NOUVELLE ORGANISATION À L'ÉPREUVE

5 DÉCEMBRE
ABOUTISSEMENT DES NÉGOCIATIONS RELATIVES AU CYBERSECURITY ACT

13 DÉCEMBRE
*L'ANSSI PARTICIPE À L'*INTERNET GOVERNANCE FORUM *ORGANISÉ À PARIS*

2019

EXERCICES ET CHALLENGES
INTERNATIONAL
RÉGULATION
POLITIQUE INDUSTRIELLE
RAYONNEMENT SCIENTIFIQUE

PRÉVENIR LES RISQUES, ANTICIPER LES USAGES

L'ANSSI s'attache à appréhender le risque et les moyens d'y répondre dans un contexte de complexification de l'écosystème numérique. Dans cette nouvelle donne, usages, services et données sont amenés à circuler et à être traités par un nombre croissant d'acteurs.

L'observation des tendances relatives aux usages numériques constitue à ce titre un champ d'étude particulièrement intéressant. Réfléchir collectivement aux tendances futures, c'est se poser les questions suivantes : quels sont les services dont nos pratiques professionnelles et personnelles ne pourront plus se passer ? Du point de vue de la sécurité, en quoi cela peut-il constituer une opportunité ou un risque ? Comment cela peut-il changer notre manière de « faire de la sécurité numérique » ?

À quelles évolutions de nos métiers, formations, méthodes et partenariats devons-nous nous préparer ?

D'une certaine manière, l'ANSSI vit déjà ce changement de paradigme. En témoignent l'extension de son champ de préoccupation des infrastructures vers les métiers ; de la défense vers l'accompagnement concomitant de la transition numérique ; du tout technique vers le développement d'expertises complémentaires devenues indispensables.

En se donnant le temps et les moyens de réfléchir aux impacts qu'auront ces tendances sur nos métiers, l'ANSSI distille tout au long de ce rapport une partie des résultats de ces travaux et invite chaque acteur à participer à ces réflexions.

SE PLACER AU CŒUR DE L'ÉCOSYSTÈME NUMÉRIQUE

TOUS CONNECTÉS, TOUS CONCERNÉS, TOUS RESPONSABLES ! L'ACCOMPLISSEMENT DE LA TRANSFORMATION NUMÉRIQUE REPOSE SUR L'IMPLICATION INDIVIDUELLE ET COLLECTIVE, À CHAQUE ÉCHELLE ET DE MANIÈRE CONTINUE. L'INSTAURATION DE LA CONFIANCE, GARANTE DU SUCCÈS DE CETTE TRANSFORMATION, REQUIERT LA PARTICIPATION DE TOUT UN RÉSEAU D'ACTEURS À ANIMER ET DÉVELOPPER.

01 // LA CONFIRMATION DU MODÈLE FRANÇAIS DE CYBERDÉFENSE

Le modèle français sur lequel repose l'activité de l'ANSSI distingue clairement les missions défensives des missions offensives et prend corps à travers le rôle d'autorité nationale de l'agence en matière de cyberdéfense et de cybersécurité. Si cette autorité repose sur une base légale indiquant quels sont les responsabilités et le périmètre d'action de l'agence, faire autorité repose notamment sur la reconnaissance de son expertise et sa capacité à entrainer et animer un réseau d'acteurs extrêmement large.

L'ÉTAT GARANT DE LA STABILITÉ DE L'ÉCOSYSTÈME

Peu importe le secteur d'activité dans lequel on se trouve, tout se transforme au contact du numérique : représentation de l'espace, métiers, usages, réglementation, économie, diplomatie, etc. Face à ce constat, la prise en compte des enjeux de sécurité numérique requiert l'engagement et la mobilisation de l'ensemble des parties prenantes, à commencer par l'État.

L'État s'engage

Le SGDSN et l'ANSSI, par le caractère unique de leurs responsabilités et leur positionnement interministériel, se voient confier de nombreuses missions par le Président de la République et le Premier ministre. En mettant à profit son expérience et son expertise, l'ANSSI participe ainsi, en collaboration avec d'autres services de l'État, à divers projets liés à la sécurité numérique et promus par les plus hautes autorités. Cet engagement démontre la volonté de la France de faire de la sécurité, gage de confiance, la condition sine qua non de la réussite de la transformation numérique.

« La France a fait de la promotion de la paix et du renforcement de la stabilité du cyberespace l'une de ses priorités. »
Guillaume Poupard,
directeur général de l'ANSSI

RÉGULER LE CYBERESPACE : UNE COOPÉRATION ENTRE ACTEURS PLURIELS

La régulation en matière de sécurité numérique consiste en la recherche d'une certaine stabilité dans le cyberespace. Elle doit rassembler et atteindre un niveau suffisant pour insuffler de la confiance chez les utilisateurs et favoriser le développement continu et harmonieux d'une société et d'une économie numériques.

L'action même du régulateur se place au carrefour de plusieurs principes indispensables à son accomplissement : une nécessaire coopération entre régulateurs et régulés, une prise en compte accrue des réalités métier, ainsi qu'une articulation entre principes nationaux et européens.

Dès lors, la régulation peut se matérialiser par la mise en œuvre différenciée ou combinée d'actions réglementaires, de sensibilisation ou de mesures d'assistance et d'accompagnement. Travailler en bonne intelligence et en confiance avec l'écosystème, suppose de maintenir un équilibre subtil entre ces trois leviers d'action.

« L'ANSSI dispose d'une capacité opérationnelle doublée d'un talent d'accompagnement qui lui permet de " justifier " l'usage de l'outil réglementaire ou normatif. »
Claire Landais,
secrétaire générale de la défense et de la sécurité nationale

Mutualiser les expertises

L'interpénétration des enjeux (économiques, éthiques, techniques, etc.) est de plus en plus forte et requiert l'implication du plus grand nombre. Cela conduit régulièrement l'agence à intervenir sur des secteurs déjà organisés qui ont leurs propres schémas de régulation, des politiques publiques, etc. Cette indispensable démarche de co-régulation entre l'ANSSI, les administrations de tutelle, les régulateurs sectoriels et les opérateurs amène l'agence à concevoir ses relations avec les différents ministères et organes gouvernementaux de manière ouverte et agile.

L'année 2018 a vu se concrétiser de nombreuses initiatives permises par une étroite coopération interministérielle. Si certaines d'entre elles concourent directement au développement sécurisé de services numériques proposés par l'État, d'autres accompagnent les nouveaux usages par l'essor d'une culture de la sécurité auprès du plus grand nombre.

Ainsi, et à l'issue de plus d'une année de travail dédiée à la conceptualisation de la méthode, le guide *Agilité et sécurité numériques : méthode et outils à l'usage des équipes projet* a rejoint la bibliothèque des développeurs en mode agile. Coréalisé par l'ANSSI et la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) et inspiré de l'expérience issue du terrain, ce guide explique de manière pratique et concrète comment l'agilité et la sécurité concourent au développement sécurisé des projets et à la gestion du risque numérique.

Incubé au sein de l'ANSSI à l'issue d'un travail interministériel associant le ministère de l'Intérieur et officiellement lancé en 2017 sous la forme d'un partenariat public-privé, le dispositif national Cybermalveillance.gouv.fr poursuit son développement. En 2018, le dispositif a rassemblé ses membres autour d'un projet commun : la création d'un kit de sensibilisation gratuit à destination des entreprises, collectivités et associations. Par le partage de son expérience et de son expertise, l'ANSSI a contribué à l'élaboration de supports d'information et de sensibilisation.

Au cœur des préoccupations des entreprises et du tissu local, les questions de sécurité économique associées aux enjeux de sécurité numérique ont continué de mobiliser l'ANSSI et ses partenaires dans un effort soutenu. À cet égard, la Direction générale des entreprises (DGE) a pris une part active dans l'essor du dispositif SecNumEco, les campagnes de sensibilisation comme le mois européen de la cybersécurité (cf. p. 41) ou encore le développement de ressources documentaires et pédagogiques.

Directive NIS : l'ANSSI accompagne les premiers opérateurs de services essentiels

Pilote de la transposition de la directive européenne *Network and Information Security* (NIS) en France, l'ANSSI a mis en place une démarche d'accompagnement progressive, ouverte et qualitative pour soutenir une vision ambitieuse. La liste des services essentiels identifiés dans le décret n° 2018-384 du 23 mai 2018 est issue de l'annexe II de la directive, de retours d'expérience du dispositif appliqué aux OIV mais également de plus d'un an de consultations menées par l'ANSSI auprès d'acteurs publics et privés ainsi que de partenaires européens.

« Ces consultations ont permis de présenter le dispositif global, recueillir les observations de chacun et aborder dans le détail la liste de services essentiels envisagée. »

Séverine Oger,
cheffe de projet transposition
de la directive NIS

La directive NIS donne l'opportunité à la France de renforcer le niveau de sécurité de nouveaux opérateurs offrant des services dans un champ économique et sociétal qui, bien qu'essentiels, échappaient à la réglementation en matière de cybersécurité.

Conformément à ses engagements, la France a identifié 122 opérateurs de services essentiels (OSE) à l'échéance du 9 novembre 2018 fixée par la directive. Ces opérateurs bénéficient de l'accompagnement des agents responsables de la coordination de l'action sectorielle de l'ANSSI. Les dossiers de désignation d'une centaine d'opérateurs additionnels sont d'ores et déjà en cours d'instruction.

LA TRANSPOSITION DE LA DIRECTIVE EN CINQ DATES CLÉS

26 février 2018
Promulgation de la loi n° 2018-133 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité

25 mai 2018
Publication du décret n° 2018-384 du 23 mai 2018

13 juin 2018
Publication de l'arrêté portant sur les modalités de déclaration des incidents

1er août 2018
Publication de l'arrêté relatif au coût des contrôles par l'ANSSI

29 septembre 2018
Publication de l'arrêté sur les règles de sécurité des OSE et leurs délais d'application

L'ÉCLAIRAGE D'ADELINE LESCAUT

CHEFFE DU BUREAU AFFAIRES JURIDIQUES, SOUS-DIRECTION ADMINISTRATION

ADELINE LESCAUT

Quelles sont les spécificités du métier de juriste à l'ANSSI ?

▼ La particularité du métier de juriste à l'ANSSI réside essentiellement dans les liaisons intrinsèques qui existent entre la sécurité des systèmes d'information et le droit. Pour pouvoir qualifier juridiquement une situation, il nous faut absolument en saisir les principes techniques, principes qui évoluent généralement plus vite que le droit… Au quotidien, nous faisons donc preuve d'agilité pour jongler avec des concepts variés auxquels s'ajoute le contexte particulier de l'administration. Se situer au carrefour de ces différentes expertises rend notre métier à la fois complexe et passionnant.

De quelle manière ton bureau a-t-il participé aux dossiers qui ont marqué l'année ?

▼ Le bureau assure une mission de conseil et d'assistance à la production de la réglementation. Plus concrètement, cela s'est traduit en 2018 par une action renforcée de conseil et de soutien dans la procédure de transposition de la directive NIS. La loi de programmation militaire (LPM) nous a, quant à elle, mobilisés de bout en bout aux côtés de la sous-direction opérations et bien au-delà de la seule année 2018. Il a d'abord fallu identifier les besoins en termes de capacités de détection puis rédiger le projet de texte que nous avons ensuite porté tout au long de la navette législative jusqu'à sa publication.

Au regard des tendances actuelles, quels sont selon toi les sujets de sécurité numérique qui, demain, attireront toute l'attention des experts juridiques ?

▼ Le rythme différencié du droit et de la technique nous oblige à fournir un effort d'anticipation permanent. L'intelligence artificielle et les villes intelligentes font partie des sujets dont de nombreux aspects doivent être prévus par le droit. Citons par exemple les principes de responsabilité des parties prenantes, d'assurance ou encore de propriété intellectuelle. La sécurité numérique appelle une mobilisation et une spécialisation renforcées des experts juridiques.

LPM 2019-2025 : la publication du décret d'application de l'article 34

L'élaboration de l'article 34 de la loi de programmation militaire 2019-2025 aux côtés des opérateurs de télécommunications s'inscrit dans une démarche vertueuse et de confiance. Tout l'enjeu de ces réflexions réside dans la volonté de tracer les contours d'un dispositif efficace capable de détecter les attaques sans porter atteinte à la vie privée des victimes potentielles en vue d'élever significativement le niveau global de sécurité numérique de la France. Le nouveau dispositif comporte deux volets bien distincts :

- Le premier volet du dispositif proposé consiste à autoriser les opérateurs de communications électroniques (OCE) à mettre en œuvre des systèmes de détection dans leurs réseaux afin de détecter les attaques informatiques visant leurs abonnés. Pour ce faire, l'ANSSI leur fournira des indicateurs de compromission (cf. ci-contre). Si l'attaque détectée concerne un opérateur d'importance vitale (OIV), un opérateur de services essentiels (OSE) ou une autorité publique, l'agence pourra alors demander des informations techniques complémentaires pour la caractériser et faire mettre en œuvre les mesures de protection et de remédiation requises.

- Le second volet du dispositif donne la possibilité à l'ANSSI, lorsqu'elle a connaissance d'une menace grave et imminente sur les systèmes d'une autorité publique ou d'un OIV, de mettre en place un dispositif de détection local et temporaire (dispositif de circonstance) sur le serveur d'un hébergeur ou l'équipement d'un OCE contrôlé par un attaquant. Le dispositif de détection est mis en œuvre pour la stricte durée nécessaire à la caractérisation de la menace. Pour aboutir, ce volet des négociations a fait l'objet d'une coordination étroite entre l'agence, les opérateurs, les hébergeurs et les législateurs pour faire se rencontrer les réalités techniques, législatives et opérationnelles. Enfin, l'ANSSI peut s'appuyer sur les OCE pour signaler aux abonnés des vulnérabilités sur leurs systèmes d'information.

« Des échanges riches et vertueux nous ont permis d'expliquer en quoi consiste notre métier. »
François Deruty,
sous-directeur opérations

Le respect du cadre juridique dans lequel s'inscrivent les nouvelles missions de l'ANSSI est contrôlé par l'Autorité de régulation des communications électroniques et des postes (ARCEP) depuis le 1er janvier 2019.

LA DÉTECTION : MAILLON ESSENTIEL DE LA CHAÎNE DE CYBERDÉFENSE

L'activité de détection repose notamment sur l'expertise et la connaissance de l'ANSSI en matière de menace stratégique et de techniques d'attaque de masse. Les experts cherchent ainsi à détecter les marqueurs techniques de certains attaquants comme l'adresse IP d'un serveur malveillant ou le nom d'un site Internet piégé. Hautement technique, cette activité implique une part importante des ressources humaines et techniques du centre opérationnel de l'ANSSI. Si la détection n'empêche pas les attaques de se produire, elle facilite leur prévention et appuie les opérations de réponse aux incidents.

CHIFFRES DE L'ACTIVITÉ DE DÉTECTION

45 859
marqueurs mis en détection

406
signalements aux bénéficiaires du service de supervision

4
déploiements de dispositifs de détection

Mesurer son exposition sur Internet

Depuis l'automne, la sous-direction opérations (SDO) réalise tous les trois mois, pour les ministères et OIV qui en font la demande, une cartographie du niveau d'exposition de leurs services et ressources sur Internet. L'objectif est de permettre une meilleure évaluation de cette exposition, de réduire la surface d'attaque sur Internet et de lutter contre le risque de compromissions. En quelques mois seulement, près de 50 bénéficiaires ont eu accès à ce nouveau service sur plus de 500 000 adresses IP scannées.

02 // UNE APPROCHE QUI PLACE L'ANSSI AU CŒUR D'UN ÉCOSYSTÈME DE CONFIANCE

La sécurité doit s'extraire de son domaine réservé pour associer l'ensemble des acteurs de la société numérique. Il en va du développement même des technologies et usages numériques dont la jouissance et la pérennité reposent sur la confiance que leur accordent les utilisateurs. Pour impliquer, développer la filière, valoriser les compétences et faire se rencontrer les expertises, l'ANSSI s'engage dans une démarche partenariale volontariste.

PARTENARIATS PUBLIC-PUBLIC

En 2018, l'ANSSI et plusieurs autorités nationales sectorielles se sont engagées en faveur d'une coopération renforcée dans le domaine de la protection des systèmes d'information par la signature commune de plusieurs lettres d'intention. L'objectif est de favoriser le développement d'une action coordonnée de tous les acteurs pour mieux répondre aux enjeux de sécurité du numérique.

Ces accords prévoient un échange régulier d'informations entre l'ANSSI et l'organisation partenaire sur les incidents affectant la sécurité des systèmes d'information, l'identification d'exigences de sécurité numérique ou encore la mise en place d'une action coordonnée en cas de crise.

Ainsi, en 2018, l'agence a conclu quatre accords de partenariat avec les organisations suivantes :

- L'Autorité de contrôle prudentiel et de résolution (ACPR) 17/01/2018
- L'Autorité des marchés financiers (AMF) 16/02/2018
- L'Établissement public de sécurité ferroviaire (EPSF) 20/03/2018
- La Direction de la sécurité de l'aviation civile (DSAC) 13/07/2018

Édouard Fernandez-Bollo, secrétaire général de l'ACPR, et Guillaume Poupard, directeur général de l'ANSSI

RENCONTRE AVEC PATRICK GANDIL

DIRECTEUR GÉNÉRAL DE L'AVIATION CIVILE (DGAC) ET PRÉSIDENT DU CONSEIL POUR LA CYBERSÉCURITÉ DU TRANSPORT AÉRIEN (CCTA)

PATRICK GANDIL

Le risque numérique est un risque à part entière qui doit être traité au plus haut niveau : de quelle manière les directions de la DGAC s'emparent-elles du sujet ?

La DGAC a un long passé de culture du risque. Appliquée au domaine numérique, une nouvelle politique de sécurité des systèmes d'information (PSSI) a été élaborée, conforme à la PSSI de l'État (PSSIE), et couvrant l'ensemble des systèmes (gestion et opérations). Une comitologie spécifique existe désormais. Placée auprès du directeur général, elle prend la forme d'une instance chargée d'analyser le risque numérique et d'organiser la stratégie de remédiation.

Au regard des tendances actuelles, comment vous organisez-vous face au risque ?

Le métier opérationnel de la DGAC – le contrôle de la navigation aérienne – repose sur des systèmes rigoureusement confinés et régulièrement audités. Malgré tous ces systèmes, le cœur du métier, c'est le savoir-faire des contrôleurs aériens. La réponse au risque n'est donc pas seulement technique : elle réside également dans la perfection des procédures et des usages. Pour l'ensemble des systèmes, la formation des agents est un axe essentiel de maîtrise du risque numérique.

L'année 2018 est celle de la création du Conseil pour la cybersécurité du transport aérien (CCTA). Quel premier bilan en tirez-vous ?

Le comité exécutif du CCTA s'est réuni deux fois en 2018, rassemblant les plus hauts décideurs du transport aérien. Le travail des comités techniques sous-jacents s'est poursuivi à un rythme soutenu, aboutissant à une production de qualité : consolidation des scénarios de menaces ; méthodologie des réponses ; liens avec les référentiels internationaux. Le CCTA est désormais l'enceinte où la cybersécurité du transport aérien s'organise et se décide.

Quels grands chantiers relatifs à la sécurité numérique mobiliseront la France et les professionnels du transport aérien pour apporter la confiance nécessaire à la croissance du secteur ?

Le transport aérien repose massivement sur les systèmes d'information. La confiance des opérateurs et la croissance de leur activité dépendent ainsi pour une part importante de la cybersécurité des flux, au sol comme en vol. Dans cette équation, le rôle du CCTA est crucial : il planifie et coordonne les travaux liés à la cybersécurité des compagnies, aéroports, constructeurs et opérateurs de la navigation aérienne.

PARTENARIATS PUBLIC-PRIVÉ

L'ANSSI souhaite fédérer l'écosystème derrière la poursuite d'un objectif essentiel : renforcer et garantir la stabilité, la prospérité et la confiance dans le cyberespace. Pour y parvenir, l'agence appelle l'ensemble des acteurs à identifier et assumer leur part de responsabilité au plus tôt. Chaque utilisateur doit devenir un acteur vigilant, aussi prudent dans l'espace numérique que dans l'espace physique.

« L'écosystème se transforme au contact de l'ANSSI et inversement. »
Emmanuel Germain,
directeur général adjoint de l'ANSSI

Parce que la transformation numérique implique de très nombreux acteurs, ces derniers doivent associer les concepteurs de produits et de solutions numériques tout comme les artisans du droit et des politiques publiques. Tous ont un rôle à jouer ; la sécurité n'est plus seulement l'affaire d'experts techniques. L'année 2018 a ainsi vu se renforcer les démarches partenariales entre acteurs publics et privés. Une dynamique à laquelle l'ANSSI souscrit depuis longtemps.

Renforcement des actions territoriales et enjeux de société

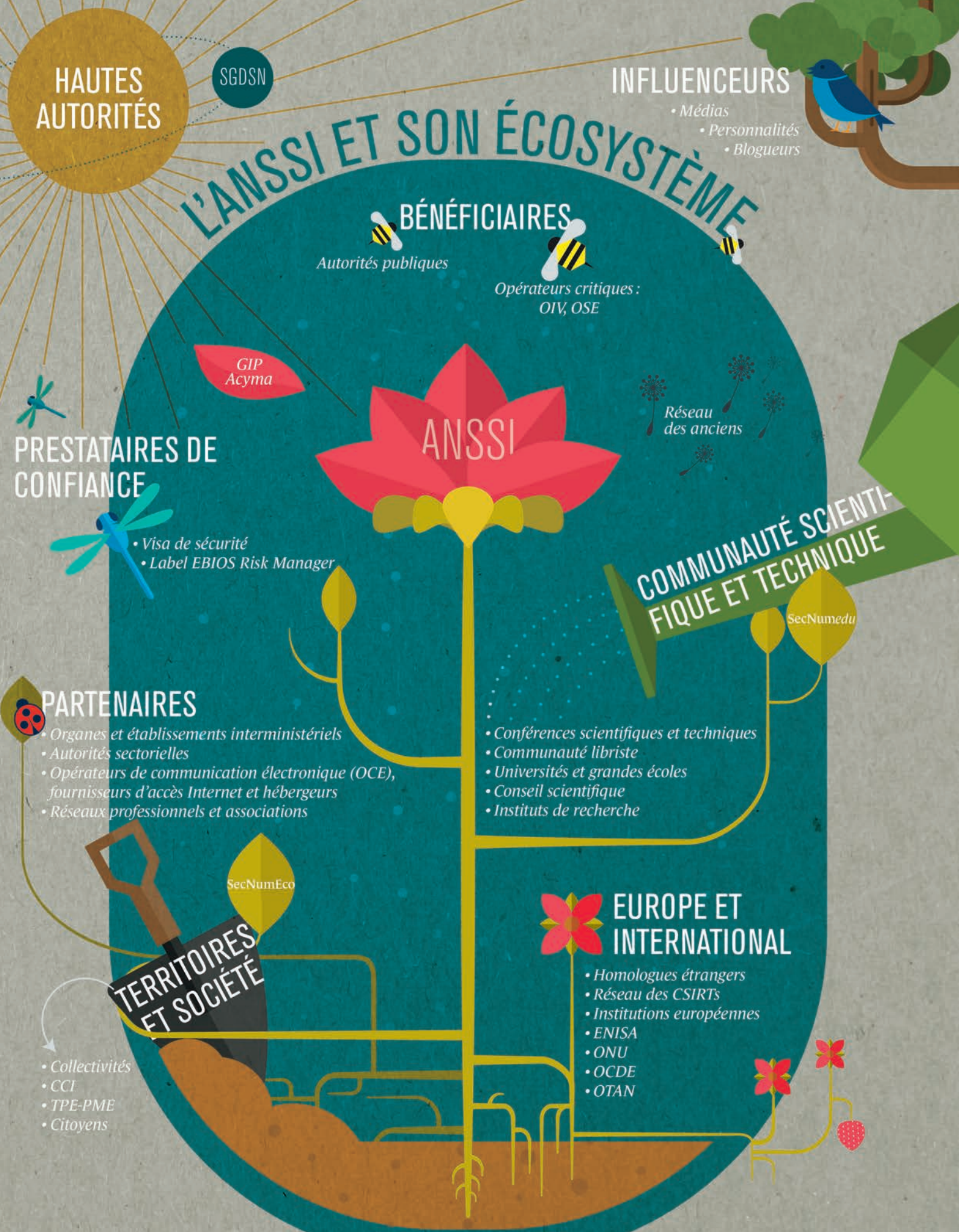
Les collectivités territoriales sont de plus en plus conscientes de leur vulnérabilité face aux risques numériques eu égard à la sensibilité des données traitées, à la variabilité des ressources ou encore au tempo réglementaire et législatif. Cette conscience est notamment aiguisée par la médiatisation des attaques survenues en 2017, l'essor des actions de sensibilisation ou encore la mise en œuvre du Règlement général sur la protection des données à caractère personnel (RGPD). Toutefois, les spécificités des collectivités territoriales rendent plus difficile l'instauration systématique et homogène d'un cadre en matière de sécurité numérique.

SecNumEco : conjuguer sécurité économique et numérique

La mondialisation des échanges économiques est source de nombreuses opportunités, mais également de nouvelles menaces. Ces risques pèsent de manière indifférenciée sur les structures publiques et privées de toutes tailles, de tous secteurs et la protection des informations ne concerne pas (ou plus) les seuls responsables de la sécurité. Dans ce contexte, la capacité des dirigeants à impliquer chaque membre de l'organisation dans la sécurité économique et numérique est un enjeu essentiel.

C'est de ce constat et du partenariat qui lie l'ANSSI au Service de l'information stratégique et de la sécurité économiques (SISSE) qu'est né le dispositif SecNumEco. Ainsi en 2018, dix rendez-vous se sont tenus à travers toute la France.

SecNumEco 2018


HAUTES AUTORITÉS
SGDSN
INFLUENCEURS
• Médias
• Personnalités
• Blogueurs
L'ANSSI ET SON ÉCOSYSTÈME
BÉNÉFICIAIRES
Autorités publiques
Opérateurs critiques : OIV, OSE
GIP Acyma
ANSSI
Réseau des anciens
PRESTATAIRES DE CONFIANCE
• Visa de sécurité
• Label EBIOS Risk Manager
COMMUNAUTÉ SCIENTIFIQUE ET TECHNIQUE
SecNumedu
• Conférences scientifiques et techniques
• Communauté libriste
• Universités et grandes écoles
• Conseil scientifique
• Instituts de recherche
PARTENAIRES
• Organes et établissements interministériels
• Autorités sectorielles
• Opérateurs de communication électronique (OCE), fournisseurs d'accès Internet et hébergeurs
• Réseaux professionnels et associations
SecNumEco
TERRITOIRES ET SOCIÉTÉ
• Collectivités
• CCI
• TPE-PME
• Citoyens
EUROPE ET INTERNATIONAL
• Homologues étrangers
• Réseau des CSIRTs
• Institutions européennes
• ENISA
• ONU
• OCDE
• OTAN

Impliquer la société civile

Les attentes des citoyens en matière de sécurité numérique se manifestent en tout premier lieu par un besoin d'information et d'implication. La conscience qu'a l'ANSSI de ces attentes prend progressivement corps à mesure que s'impose la nécessité de responsabiliser le plus grand nombre. De premières initiatives ont ainsi vu le jour en 2018 comme l'espace de réflexion baptisé Agora 41 (cf. p. 47), l'essor de multiples formes de consultations ou encore la présence grandissante de l'agence dans la communauté Open Source (cf. p. 45).

Former pour expliquer, transmettre et responsabiliser

La sécurité numérique est encore peu présente dans les cycles de formation continue. Conscient de cet axe de progrès, le Centre de formation à la sécurité des systèmes d'information (CFSSI) de l'ANSSI a lancé le programme SecNum*edu*-FC qui compte 16 formations labellisées. Ce programme vient compléter le label SecNum*edu* pour les formations initiales en cybersécurité de l'enseignement supérieur. Avec 11 nouvelles formations distinguées en 2018, le réseau SecNum*edu* en compte désormais 52. CyberEdu, qui incorpore quant à lui un volet sécurité numérique dans les formations en informatique, a distingué cinq nouvelles formations au cours de l'année.

SECNUMEDU-FC, LE PETIT DERNIER DE LA FAMILLE EDU

Lancé à titre expérimental au début de l'année 2018, le label SecNum*edu*-FC (pour « formation continue ») référence les formations continues dédiées à la sécurité numérique (formations courtes de quelques jours à quelques semaines). Il s'adresse aux salariés, employés ou demandeurs d'emploi qui souhaitent améliorer ou acquérir des compétences professionnelles en matière de sécurité numérique. Le label permet en outre d'éclairer les choix des employeurs en matière de formation continue. Attribué pour une durée de 3 ans, il rassemble des formations continues dédiées à hauteur de 70 % au moins à la sécurité numérique.

Enfin, le programme de sensibilisation en ligne SecNum*académie* détenteur du prix « Coup de cœur des internautes » 2018 (cérémonie MOOC of the year) enregistre 78 500 inscriptions depuis sa création. Le succès de l'initiative vient confirmer les attentes des citoyens dans ce domaine. Pour en faire bénéficier le plus grand nombre, il est primordial d'étoffer la place de la sécurité numérique à l'école en fournissant aux professeurs les ressources pédagogiques nécessaires. Une véritable volonté politique incite à poursuivre dans cette voie en vue de réaliser un double objectif : une meilleure sensibilisation de la population et la naissance de vocations pour les métiers liés à la cybersécurité.

Données au profit des personnels de l'État, les formations dispensées par le CFSSI sous forme de stages courts ou d'un cycle long menant à l'obtention du titre d'expert en sécurité des systèmes d'information (ESSI) ont pour leur part accueilli 1 329 personnes en 2018, ce qui représente près de 2 500 heures de formation cumulées.

« La sécurité numérique doit faire son entrée dans les manuels scolaires et la formation professionnelle, pour faire de chacun un acteur engagé. »
Guillaume Poupard,
directeur général de l'ANSSI

L'ANSSI remet ses premiers Visas de sécurité

Avec la création du Visa de sécurité, l'ANSSI donne une meilleure lisibilité à l'offre de solutions et de services numériques sécurisés. Si la remise des Visas le 14 juin 2018 en présence du secrétaire d'État chargé du numérique a largement participé à la promotion du dispositif, il convient désormais de l'étendre. Dans ce cadre, faciliter l'accès aux savoir-faire dont disposent les acteurs de la filière en participant à accentuer la visibilité de solutions d'excellence constitue un enjeu déterminant.

CERTIFICATIONS

25 certifications de sécurité de premier niveau (CSPN) de produits

68 certificats critères communs (CC) de produits

12 certificats CC de sites

3 certificats CC de profils de protection

QUALIFICATIONS

15 produits

36 prestataires

CENTRES D'ÉVALUATION AGRÉÉS

15 centres d'évaluation de la sécurité des technologies de l'information (CESTI) de services

174 VISAS REMIS EN 2018

Le Cloud à l'épreuve de la confiance

SecNumCloud

L'ANSSI a initié le projet de référentiel à destination des prestataires de services informatiques en nuage (Cloud) en 2014. En juin 2018, le référentiel a évolué avec une mise à jour majeure : l'intégration d'éléments du RGPD. Ce travail en collaboration avec la CNIL fait de la qualification SecNumCloud le premier référentiel européen proposant une première étape de conformité au RGPD.

RGPD – RENFORCER LA SÉCURITÉ DES DONNÉES À CARACTÈRE PERSONNEL

À l'occasion de l'entrée en application en mai 2018 du Règlement général sur la protection des données (RGPD), l'ANSSI a mis à disposition des entités publiques et privées concernées un « kit de la sécurité des données ». Relayé par la CNIL, il accompagne ces entités dans le renforcement de la sécurité des données à caractère personnel qu'elles sont amenées à traiter.

Stratégie Cloud de l'État

La circulaire n° 6049-SG du 8 novembre 2018 est un document structurant de portée nationale sur l'informatique en nuage. Née d'une collaboration étroite entre acteurs, elle invite au développement d'une offre composée de trois cercles de solutions. Les solutions rassemblées dans chacun de ces cercles le sont en fonction de l'usage qui est fait de la technologie et du niveau de sensibilité des données traitées et applications adjacentes.

Ainsi, le « Cloud interne » correspond aux Cloud interministériels dont le développement se poursuit au sein de certains ministères. Le « Cloud dédié » correspond à une offre de Cloud réalisée et exploitée par un industriel du secteur. Le « Cloud externe » correspond quant à lui aux offres de Cloud externes génériques accessibles sur Internet et dont le catalogue sera porté par des centrales d'achat pour en faciliter la commande. La conformité au référentiel SecNumCloud sera exigée dans le cas des Cloud internes et dédiés et fortement recommandée dans le cas des Cloud externes.

OÙ COMMENCENT ET S'ARRÊTENT LES SYSTÈMES D'INFORMATION ?

Les acteurs du numérique évoluent désormais au sein d'un cyberespace vaste et complexe à défendre, dénué de frontières géographiques, politiques et même parfois techniques. Cette réalité nous confronte à un phénomène de perte de notion du périmètre du système d'information.

En grande partie liée à l'apparition ou au renforcement de certains usages, cette tendance s'explique notamment par le développement de l'externalisation des données (exemple : Cloud), une plus grande ouverture des systèmes sur Internet, un essor du nomadisme (exemple : télétravail) ou encore l'interconnexion quasi-systématique des systèmes (exemple : objets connectés).

Au cœur de cette mutation se pose la question de la confiance. Plus difficile à évaluer que la seule sécurité, la confiance dans des infrastructures de type Cloud ne peut s'envisager que dans la durée. Les réponses actuellement apportées consistent essentiellement en l'isolation des systèmes les plus sensibles. Cette approche atteint ses limites et doit conduire à la mise en œuvre d'initiatives qui ne seront porteuses de sens et de résultats qu'à l'échelle européenne.

L'instauration de la confiance en ces solutions doit, selon l'ANSSI, s'attacher à instruire plusieurs champs d'action :

- réduire les risques liés à la migration des données dans le Cloud par une attention renforcée à l'égard des processus critiques et l'intervention du législateur européen ;
- accompagner le phénomène de « dépérimétrisation » du système par la recherche d'un équilibre entre fonctionnalité et fermeté ;
- s'adapter au déplacement de la sécurité des systèmes vers la sécurité de l'information et des services numériques par un accompagnement au changement à la fois culturel et opérationnel.

03 // LA FRANCE, MOTEUR DE LA SÉCURITÉ DU NUMÉRIQUE EN EUROPE

La France et l'Europe ont un rôle majeur à jouer pour endiguer le développement d'un Far West numérique. L'Appel de Paris pour la confiance et la sécurité dans le cyberespace, lancé en novembre dernier par le Président de la République, permet de tracer une voie crédible en ce sens.

« Il est essentiel de se mettre d'accord à l'échelle internationale sur ce qu'il est permis ou non de faire dans le cyberespace. »
Guillaume Poupard,
directeur général de l'ANSSI

L'Appel de Paris invite États, organisations et société civile à s'engager

Les attaques de grande ampleur comme celles qui ont marqué l'année 2017 ont révélé les contours d'une réalité encore mal perçue : la sécurité numérique doit être élevée au rang de priorité stratégique tant les enjeux économiques, de paix et de stabilité dans le cyberespace sont importants. Pour relever ce défi, une responsabilité nécessairement partagée en matière de sécurité numérique entre États, utilisateurs et acteurs économiques doit s'affirmer.

« Je crois très profondément qu'il y a urgence. Urgence à ce que nous, acteurs multiples du fonctionnement de l'Internet, prenions en main ces sujets en acceptant toutes nos responsabilités à cet égard. »
Emmanuel Macron,
Président de la République française
Discours de l'Appel de Paris

La responsabilité des acteurs privés

Suite à la publication de la Revue stratégique de cyberdéfense (RSC) le 15 mars 2018, le ministère de l'Europe et des affaires étrangères et l'ANSSI ont défini l'ambition française visant à préciser et renforcer les responsabilités des acteurs privés quant à la stabilité du cyberespace. La France défend le besoin de clarifier et de partager un vocabulaire et des concepts communs sur des problématiques comme le *hackback* afin d'en définir les limites. Une « zone d'incertitude » existe aujourd'hui, porteuse d'instabilité et de flou juridique, qu'il est nécessaire de considérer aussi bien au niveau national qu'au niveau international, tant pour les acteurs privés que pour les services de l'État.

« La France a su saisir une opportunité qui s'offrait à elle pour promouvoir la paix dans le cyberespace via un ensemble d'idées qui préexistaient isolément. »
Yves Verhoeven,
sous-directeur stratégie

L'absence d'obligations pour les acteurs privés de concevoir et de maintenir des solutions numériques à l'état de l'art en termes de sécurité vient également accroître le risque de déstabilisation à l'échelle internationale. Il est essentiel de prendre conscience de la portée systémique de ces risques pour amener les acteurs non-étatiques à s'emparer de ces sujets, sans freiner les bénéfices de la transition numérique.

Portée à l'échelle interministérielle, la RSC a donné naissance au centre de coordination des crises cyber (C4). À travers lui, la Revue insiste sur la nécessité de se réunir régulièrement pour traiter collectivement et au niveau stratégique les questions de cyberdéfense.

RENCONTRE AVEC NICOLAS ROCHE

DIRECTEUR DES AFFAIRES STRATÉGIQUES, DE SÉCURITÉ ET DU DÉSARMEMENT AU MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

NICOLAS ROCHE

Dans quelle mesure les coopérations bilatérales peuvent-elles participer à la prévention des crises cybernétiques ?

▼ Prévenir les crises dans le cyberespace est au cœur de notre cyberdiplomatie. Pour cela, le développement de nos coopérations à tous les niveaux (politique, technique, opérationnel, structurel, etc.) est primordial. Développer le dialogue et les échanges avec nos partenaires, dans un cadre bilatéral mais aussi multilatéral, comme à l'UE, à l'OSCE ou à l'OTAN, permet de créer de la confiance, de mettre en place des canaux pour gérer les tensions et d'élever le niveau général de résilience et de protection dans le cyberespace. Le MEAE, sous la direction de l'Ambassadeur pour le numérique, y prend toute sa part, en lien avec l'ensemble des administrations concernées.

De nouveaux dispositifs comme le C4 ont vu le jour et créent de nouveaux espaces de dialogue. Près d'un an après leur mise en fonctionnement, quels en sont les premiers enseignements ?

▼ Le C4, pour « centre de coordination des crises cyber », s'est rapidement imposé comme un rendez-vous privilégié de la « communauté cyber » française permettant d'échanger sur la menace et de préparer des stratégies de réponse globale. Le C4 permet de mieux articuler les outils à disposition de l'État pour prévenir, détecter, gérer et répondre aux attaques informatiques.

La notion de « Far West numérique » revient régulièrement : comment lutter collectivement contre cette tendance ?

▼ Certains acteurs malveillants ont rapidement perçu l'opportunité des spécificités de l'espace numérique (anonymat, accessibilité, etc.) pour servir leurs intérêts. Pour autant, dans le cyberespace, comme ailleurs, le droit international s'applique et des normes viennent encadrer le comportement des différents acteurs. Nous devons aujourd'hui œuvrer pour promouvoir et défendre ce cadre juridico-normatif, encore en cours de consolidation. C'est le sens de l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, lancé en novembre par le Président de la République et soutenu par plus de 500 entités, dont 64 États.

Cybersecurity Act : donner le *LA* en Europe

Le *Cybersecurity Act* est un règlement européen qui a fait l'objet d'intenses négociations tout au long de l'année 2018. L'ANSSI y a pris une part active. L'objectif du règlement est double :

- adopter un mandat permanent pour l'agence européenne pour la cybersécurité (ENISA) en renforçant ses missions dans plusieurs domaines : développement et mise en œuvre des politiques européennes, expertise, construction capacitaire, soutien à la coopération opérationnelle et sensibilisation ;

« Ce nouveau mandat doit inaugurer une nouvelle ère, celle d'une agence européenne partenaire des agences nationales et de leurs écosystèmes pour le passage à l'échelle de la cybersécurité européenne. »
Jean-Baptiste Demaison, président de l'ENISA et chargé de mission numérique à l'ANSSI

- définir un cadre permettant la reconnaissance mutuelle des certificats délivrés au sein de l'Union européenne (UE). Le règlement permet d'harmoniser les méthodes et la portée de la certification afin de garantir une approche cohérente des États membres de l'UE en la matière. Ce cadre précise les rôles et responsabilités respectives des États membres, de la Commission européenne et de l'ENISA.

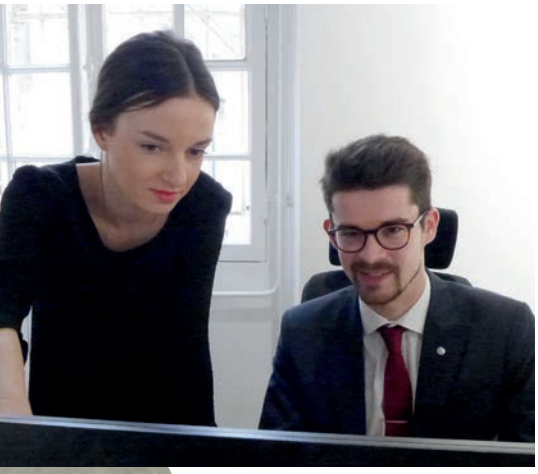
Après un an de négociation, le Conseil de l'UE, le Parlement européen et la Commission européenne sont parvenus à un accord politique début décembre 2018. Le règlement a intégré plusieurs des postures exprimées par les autorités françaises, actant ainsi :

- un mandat permanent pour l'ENISA, agence européenne dont le rôle de facilitateur des échanges entre États membres est pleinement valorisé ;

- un cadre européen de certification de sécurité tirant pleinement bénéfice des 20 ans d'expérience de certains États membres – parmi lesquels la France – et permettant d'harmoniser les approches entre ces États, sans pour autant réduire le niveau de sécurité.

L'ÉCLAIRAGE D'AMÉLIE PERRON ET VICTOR CAMBAZARD

CHARGÉS DE MISSION AFFAIRES POLITIQUES EUROPÉENNES ET INTERNATIONALES, SOUS-DIRECTION STRATÉGIE



AMÉLIE PERRON
VICTOR CAMBAZARD

Au sein de l'ANSSI, de quelle manière ont été préparées les négociations qui ont jalonné l'année ?

Amélie : L'ANSSI a toujours plaidé pour que l'UE se dote d'un cadre européen de certification de sécurité. En cela, nous étions satisfaits que la Commission européenne propose l'édiction d'un tel cadre à 28 États membres. Un an avant le début des négociations, nous nous y préparions déjà pour définir avec la division produits et services de sécurité de l'ANSSI notre vision du cadre européen de certification. Quand les négociations ont débuté, à partir de janvier, les cycles d'amendements ont tenu un rythme très soutenu. Nous avons construit notre position en étroite coopération avec l'Allemagne, dont l'approche est voisine de la nôtre. Concrètement, cela s'est traduit à chaque cycle de négociations par la proposition d'amendements communs.

Victor : Le conseil d'administration de l'ENISA étant actuellement présidé par un représentant français, nous disposions du recul nécessaire pour envisager les évolutions du mandat de l'agence, certes en faveur d'une plus forte implication des États membres dans ses activités, mais surtout afin que l'agence soit porteuse d'une véritable « valeur ajoutée européenne ». De nombreux États membres partageaient notre vision en faveur d'un renforcement de ses missions principales.

Quelle place occupent les Visas de sécurité délivrés par l'ANSSI dans ce nouveau cadre européen ?

Amélie : Les Visas de sécurité que délivre l'ANSSI sont une garantie de traçabilité. Le cadre européen de certification reprend les grands fondamentaux de la certification de cybersécurité telle que pratiquée en France depuis plus de 20 ans. L'entrée en vigueur du cadre est donc une bonne nouvelle pour les centres d'évaluation de la sécurité des technologies de l'information (CESTI) français, déjà au niveau requis, mais également pour les entrants en certification qui vont ainsi gagner un avantage compétitif à l'échelle européenne.

L'année 2019 s'ouvre sur l'adoption du règlement. De quelle manière la France va-t-elle accompagner cette entrée en vigueur ?

Amélie : La mise en place du cadre de certification amène plusieurs enjeux. D'abord, chaque État doit nommer une autorité nationale de certification. Celle-ci aura pour mission de superviser l'émission des certificats émis sur son territoire. Son contrôle sera renforcé pour le niveau d'assurance élevé, afin d'offrir plus de garanties à l'utilisateur. S'ajoute à cela la création d'un groupe européen des autorités nationales, chargé de définir les priorités européennes et de rédiger les schémas de certification européens. L'ANSSI sera particulièrement active dans la mise en place du cadre, afin de créer une communauté de premier ordre en matière de certification de sécurité.

Victor : La restructuration de l'ENISA et le renforcement de l'implication des États membres suggèrent que ces derniers doivent être les garants des travaux développés par l'agence. Cela pourra notamment s'effectuer via le nouveau réseau des officiers de liaison nationaux. Il servira à optimiser les liens entre les autorités nationales et l'agence européenne. Sur le renforcement de sa capacité de soutien à la coopération opérationnelle, le règlement acte que l'ENISA n'a pas vocation à se substituer aux compétences nationales mais qu'elle a pour mission de soutenir le développement capacitaire des États membres.

2 CULTIVER SA SINGULARITÉ

PAR LE CARACTÈRE UNIQUE DE SON MODÈLE, DE SES MISSIONS ET, SURTOUT, DES AGENTS QUI L'ANIMENT, L'ANSSI ARBORE UN PROFIL ORIGINAL DANS LE PAYSAGE INTERMINISTÉRIEL. EN 10 ANS D'EXISTENCE, L'AGENCE A SU FAIRE DE CE PROFIL HYBRIDE ET ATYPIQUE UN ATOUT QUI LUI PERMET D'ÊTRE COMPRISE ET ÉCOUTÉE DE NOMBREUX PUBLICS.

01 // UNE IDENTITÉ COMPLEXE

Ce que l'on perçoit de l'agence depuis l'extérieur est souvent le reflet de ce qu'il s'y passe à l'intérieur. C'est dans la diversité des profils et compétences de ses agents que l'ANSSI puise son agilité et son expertise.

PORTRAIT-ROBOT

La cybersécurité constitue, pour qui s'y implique, un champ d'innovation passionnant ! Profondément transdisciplinaire, elle fait interagir une grande variété d'acteurs privés et publics, en France comme à l'international. Dynamique et d'une grande richesse scientifique, la sécurité numérique pose des défis intellectuels majeurs pour les innovateurs de tous horizons.

Ce constat, s'il vaut pour un vaste écosystème, prend une forme très concrète au sein même de l'ANSSI où se côtoient des femmes et des hommes qui se distinguent par la diversité de leurs profils et expertises. Ainsi, la plasticité de l'agence s'éprouve depuis l'intérieur et offre un terreau favorable aux parcours de carrière, à l'émergence de nouveaux champs d'expertise – parfois même de nouveaux métiers – et au développement des fonctions d'encadrement.

CHIFFRES 2018

568
agents

22 %
de femmes

37 ANS
d'âge moyen

79 %
de contractuels
14 % fonctionnaires
et 7 % militaires

VIE À L'AGENCE

Valeurs : des qualités proclamées et incarnées

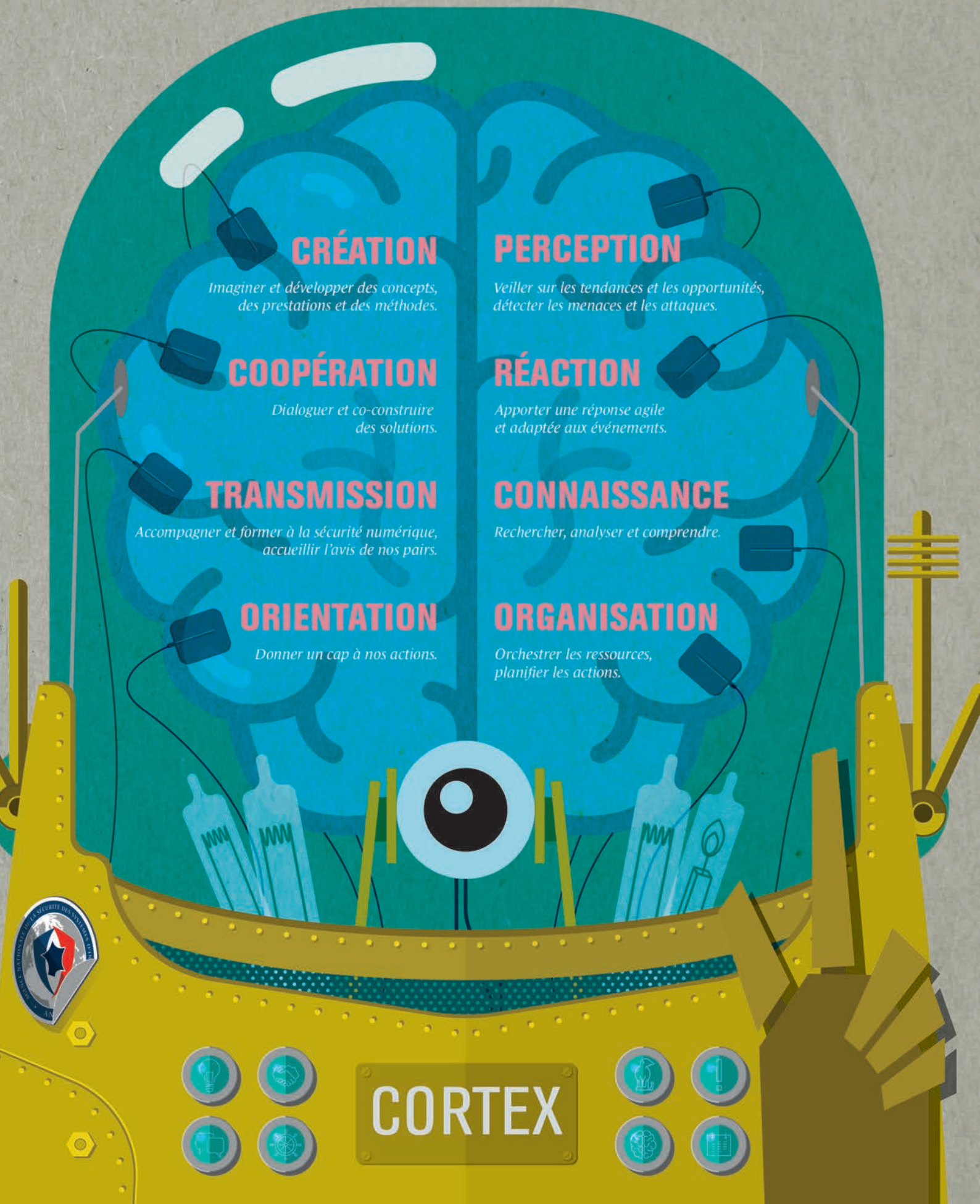
Une culture commune anime l'ANSSI. Y règnent une ambiance, des codes, des rituels, un attachement fort à la mission d'intérêt général que poursuit l'agence. Alors que celle-ci voit son périmètre d'action s'enrichir de nouvelles prérogatives et qu'un nombre croissant de profils s'y côtoient, l'identification collective des grands principes qui donnent un sens à son action est essentielle.

« L'approche participative adoptée et appréciée a fait de la réflexion sur les valeurs un moment marquant de l'année. »
Valérie Godin,
sous-directrice adjointe
administration

Les valeurs d'ouverture, d'agilité et de compétence partagées en interne sont un repère qui surpasse les évolutions que connait l'agence, dans et hors les murs. En 2018, ces valeurs et les qualités qu'elles recouvrent ont pris vie à l'issue d'une réflexion à laquelle de nombreux agents ont participé avec enthousiasme. Le livret interne issu de cette démarche a donné la parole aux agents qui y ont exprimé ce que chacune d'elles leur inspire et la manière dont ces valeurs sont incarnées au quotidien.

Formation : transmettre et recevoir

Au centre de formation à la sécurité des systèmes d'information (CFSSI), ce sont les experts de l'ANSSI qui dispensent les formations. Si l'immense majorité des formations délivrées par le CFSSI lui-même ou par les organismes partenaires ont trait à la sécurité des systèmes d'information, l'agence souhaite donner davantage d'importance aux formations en langues étrangères, conduite de projet et management.


CRÉATION
Imaginer et développer des concepts, des prestations et des méthodes.
PERCEPTION
Veiller sur les tendances et les opportunités, détecter les menaces et les attaques.
COOPÉRATION
Dialoguer et co-construire des solutions.
RÉACTION
Apporter une réponse agile et adaptée aux événements.
TRANSMISSION
Accompagner et former à la sécurité numérique, accueillir l'avis de nos pairs.
CONNAISSANCE
Rechercher, analyser et comprendre.
ORIENTATION
Donner un cap à nos actions.
ORGANISATION
Orchestrer les ressources, planifier les actions.
CORTEX

Partage et lisibilité de l'information : une préoccupation de tous les instants

Avec 568 agents répartis sur deux sites et un besoin d'interaction permanente entre sous-directions, l'ANSSI a développé des outils et des rituels internes devenus incontournables pour informer, débattre, partager et valoriser.

Créer des espaces de dialogues

Chaque année, l'agence produit et édite près de 80 publications, (cf. p.52) toutes catégories confondues (guides, articles scientifiques, référentiels, etc.). Le comité éditorial de l'ANSSI veille à leur cohérence vis-à-vis de la doctrine de l'agence, identifie les besoins, les priorise et mobilise les expertises nécessaires à la réalisation de ces productions. Composé de représentants de chaque sous-direction, le comité se réunit tous les deux mois pour échanger sur les projets en cours et veiller à la bonne circulation de l'information.

« Ces débats internes nous préparent à ceux qui nous attendent hors les murs. »
Vincent Strubel,
sous-directeur expertise

Après plus de deux années de fonctionnement, le modèle du comité éditorial a inspiré d'autres initiatives. Ainsi, le comité dédié aux profils de fonctionnalités et de sécurité (PFS) s'est réuni pour la première fois en avril 2018 pour définir avec précision les spécifications techniques des produits et services et soutenir l'industrie en vue d'atteindre les standards attendus.

Valoriser les prestations

L'ANSSI développe une offre de produits et de services (documentation, formation, projets en Open Source, etc.) qu'elle met gratuitement à la disposition de ses publics. Pour positionner cette offre et lui apporter davantage de lisibilité, le bureau qualité de la sous-direction administration a initié une démarche de valorisation des produits et services.

À terme, l'objectif est de disposer d'un catalogue de prestations en vue d'apprécier qualitativement et quantitativement chacune d'elles, d'affecter les ressources le plus justement possible, de disposer d'outils adéquats pour présenter l'activité et de renforcer l'intérêt à l'égard de ces services. En 2018, plusieurs initiatives ont bénéficié de cet accompagnement et de cette analyse parmi lesquelles la méthode d'analyse de risques EBIOS Risk Manager (cf. p. 9) ou encore CLIP OS (cf. p. 45).

AGILITÉ ET PLASTICITÉ

Organisation interne

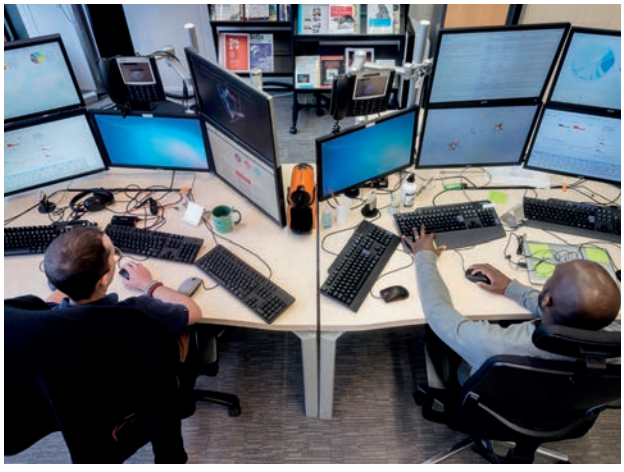
Le COSSI change de nom et de rythme

En 2018, le centre opérationnel de la sécurité des systèmes d'information (COSSI) change de nom et devient la sous-direction opérations (SDO). Derrière ce changement d'appellation, ce sont de profondes évolutions structurelles et organisationnelles qui s'opèrent. En s'appuyant sur son expérience et l'analyse des tendances que semble suivre la situation opérationnelle, SDO a mené de longs mois de réflexion en impliquant ses partenaires, les autres sous-directions de l'ANSSI et, surtout, ses propres agents qu'elle a largement associés à cette démarche.

« L'ANSSI n'a jamais cessé de se transformer. Mais aujourd'hui, peut-être est-elle en train de se réinventer à un moment qui semble opportun pour le faire. »
François Deruty,
sous-directeur opérations

Ainsi SDO s'est réorganisée de telle sorte qu'à chacune de ses divisions corresponde une famille de prestataires qualifiés. Cette correspondance illustre la volonté de l'agence d'offrir davantage de lisibilité à ses missions et relations avec l'écosystème tout en ayant à cœur d'atteindre un seuil capacitaire critique dans chacun des grands domaines.

- Division connaissance et anticipation > Prestataires d'audit de la sécurité des systèmes d'information (PASSI)
- Division détection > Prestataires de détection d'incidents de sécurité (PDIS)
- Division réponse > Prestataires de réponse aux incidents de sécurité (PRIS)



L'ÉCLAIRAGE DE FRÉDÉRIQUE BAJAT

CHEFFE DE BUREAU SITUATION ET RÉGULATION, SOUS-DIRECTION OPÉRATIONS

FRÉDÉRIQUE BAJAT

Peux-tu nous expliquer en quoi consiste ta mission ?

Le bureau situation et régulation est né d'un besoin de suivi et d'analyse de la réponse apportée par l'agence aux attaques qu'elle traite. Notre objectif est de fournir une vue globale et synthétique de ces incidents. Elle est enrichie par un travail de corrélation et de contextualisation, dans un objectif d'aide à la prise de décision ou de développement de nos partenariats. La création d'un bureau dédié à ces missions a permis de répondre à cette nécessité avec un maximum de réactivité et d'efficacité opérationnelle.

Quels sont les principaux interlocuteurs de ton équipe au sein de l'ANSSI et en dehors ?

Mon équipe travaille étroitement avec les différents experts métiers de l'agence – principalement techniques – en charge de répondre aux attaques informatiques. Nos travaux d'analyse sont ensuite transmis aux décideurs et partenaires nationaux et internationaux de l'ANSSI.

Quel regard portes-tu sur les menaces, tendances et évolutions que pourraient connaitre vos métiers ?

Les attaquants se montrent particulièrement créatifs pour faire évoluer et intensifier la menace, en parallèle de l'évolution des technologies et usages numériques. Pour y faire face, l'agence fait évoluer l'ensemble de ses métiers et modes d'intervention. Cela passe par une restructuration des opérations de détection et de réponse et une coordination renforcée avec de nombreux acteurs, internes et externes.

Parce que la gestion des opérations s'est professionnalisée, cette réorganisation est apparue comme un prérequis à la bonne poursuite des missions de l'agence. Mais se réorganiser ne suffit pas ; encore faut-il éprouver et valider ces choix.

Un retour d'expérience interne a permis d'évaluer en situation réelle la manière dont se géraient les opérations ou encore la circulation de l'information avec cette nouvelle configuration. L'exercice *Handspinner* organisé en novembre est venu compléter cette mise à l'épreuve. Véritable test opératif et technique, *Handspinner* a permis à l'agence de mesurer la capacité de cette nouvelle organisation à rapprocher son mode de fonctionnement quotidien de celui qui prévaut en temps de crise.

La CAC, interface opérationnelle

Placée auprès de la direction générale, la cellule d'anticipation cyber (CAC) a vu le jour fin 2017. Elle assure la fonction de conseil dans le domaine des opérations de cyberdéfense. En matière d'anticipation et de planification stratégiques opérationnelles, elle coordonne les travaux et pilote les sujets nécessitant une attention permanente de la direction. Pour ce faire, elle peut se saisir des questions jugées essentielles du point de vue des affaires opérationnelles.

Pour mener à bien sa mission, la CAC s'appuie sur deux outils principaux : les directives initiales de planification (DIP) et les dossiers thématiques d'anticipation (DTA). Le premier est réactif et vient en aide à la décision en proposant des objectifs et des options ; en identifiant des modalités d'engagement ; et en assurant un suivi lors de l'opération. Le second intervient quant à lui de manière proactive en prévision d'engagements futurs. Dans ce cadre, les DTA proposent une analyse de la situation assortie de postures pour l'agence. En 2018, la CAC s'est ainsi intéressée à de grands événements tels que les jeux olympiques d'hiver ou les élections européennes.

Une ambition stratégique transverse et assumée : se réapproprier le futur dans un environnement toujours plus incertain

Elle aussi rebaptisée, la sous-direction relations extérieures et coordination (RELEC) est devenue, fin 2018, la sous-direction stratégie (SDS). Cette transformation s'inscrit dans un contexte très dynamique et exigeant, rythmé notamment par des actualités fortes sur le plan national comme à l'international, dans les domaines opérationnels, techniques mais également réglementaires, stratégiques et politiques. En effet, ces dernières années ont vu les questions liées à la sécurité du numérique prendre de plus en plus d'ampleur et sortir de la stricte sphère technico-opérationnelle, terreau historique de l'agence. Cette dernière, dans sa globalité et via l'animation de SDS, est ainsi un acteur central de l'élaboration et de la mise en œuvre des politiques publiques en matière de sécurité du numérique.

La création d'une sous-direction stratégie à l'ANSSI est un élément de réponse à ces enjeux, toujours croissants, qui emportent par ailleurs de réels besoins de pilotage stratégique pour l'agence. Préserver sa liberté d'action, réduire autant que possible l'incertitude, fixer des caps clairs pour ses agents, maîtriser au mieux les contingences externes, produire des stratégies délibérées et formalisées : tels sont les objectifs du processus de planification stratégique de l'ANSSI.

À cet égard, l'année 2018 a également vu naître le comité directeur de la stratégie, permettant à l'agence de réfléchir, de manière transverse et collective, à son identité, à son modèle, à l'écosystème et aux défis qui sont les siens dès à présent et qui l'attendent dans le futur. Enfin, une cellule de planification stratégique a vu le jour fin 2018 au sein de SDS, destinée à coordonner les travaux d'élaboration et de mise à jour de la stratégie de l'agence. Par souci de cohérence, elle joue également un rôle de conseil interne au profit des autres entités de l'ANSSI auxquelles elle propose des prestations d'assistance dans l'élaboration des différentes stratégies d'activité.

Infrastructure

Datacenter : des moyens à la mesure des besoins

La mise en service du datacenter du SGDSN assortie de la migration de premiers services vers l'infrastructure a marqué l'année et, surtout, la manière dont les agents entrevoient la réalisation de leurs missions. Engagée en 2015, il a fallu deux années et près de trente agents pour superviser la construction du datacenter. Depuis, les efforts se concentrent sur l'amélioration de la qualité globale de service, la résilience des moyens de communication et la disponibilité des services.

« La construction du datacenter a beaucoup mobilisé en interne et crée une nouvelle dynamique dans nos méthodes de travail. »
Marc Yolin,
sous-directeur numérique

Particulièrement concernée par ce changement, SDO voit ainsi ses capacités de traitement augmenter dans le cadre de ses activités de détection ou encore d'audit. Pour la sous-direction, le challenge consiste désormais à gérer de manière fluide des volumes importants de données pour favoriser le bon déroulement des opérations.

L'ÉCLAIRAGE D'YVES AUGER

ARCHITECTE DE SYSTÈMES D'INFORMATION, SOUS-DIRECTION NUMÉRIQUE

YVES AUGER

Longue et complexe, la mise en œuvre du datacenter a beaucoup mobilisé en interne. Que retiens-tu de cette expérience ?

▼ Le projet a débuté en 2015 avec la construction « physique » du datacenter mais c'est aujourd'hui que l'aventure commence vraiment ! Depuis près d'un an et demi, nous avons travaillé avec toutes les sous-directions de l'ANSSI à la refonte de notre infrastructure informatique afin d'utiliser au mieux ces nouvelles capacités d'hébergement. Désormais, il nous faut déplacer ou reconstruire progressivement les services IT tout en garantissant la continuité opérationnelle aux utilisateurs.

Quels sont les principaux enjeux de sécurité d'une telle infrastructure ?

▼ Construire un datacenter de ce niveau-là, c'est rare. D'autant plus que nous ne l'avons pas construit seuls, mais avec le ministère de l'Intérieur. S'il exploite une partie de l'infrastructure, seul l'espace est partagé, sans adhérence entre nos activités respectives. C'est pourquoi nous nous sommes fait accompagner sur sa construction et son exploitation. L'enjeu ne résidait pas tant dans la sécurité puisque c'est notre cœur de métier et qu'elle a été prise en compte dès le départ, notamment dans le choix du site. En revanche, la résilience et l'évolution des services hébergés sont au cœur de nos préoccupations afin de répondre toujours mieux aux besoins croissants du SGDSN.

Après t'être longuement investi dans ce projet, quels sont tes prochains défis au sein de l'agence ?

▼ Se doter d'une infrastructure d'hébergement performante était indispensable mais cela ne suffit pas à la transformation numérique du SGDSN. La prochaine étape consistera probablement à faire évoluer la gouvernance au sein du secrétariat général pour que le système d'information puisse s'adapter aux enjeux actuels et futurs de nos métiers.

02 // SOUTENIR UNE VISION ET L'EXPLIQUER

L'ANSSI concentre ses efforts sur la sécurité des systèmes dont elle a la responsabilité et l'accompagnement de la transformation numérique pour qu'elle soit créatrice de confiance et d'opportunités.

AMENER LES AUTORITÉS À DEVENIR DES AMBASSADEURS DE LA SÉCURITÉ NUMÉRIQUE

Moyens de communication sécurisés

L'ANSSI met à disposition des hautes autorités de l'État des moyens de communication adaptés à la sensibilité des données qu'elles sont amenées à traiter. La conception de ces solutions repose sur un cahier des charges alliant disponibilité, résilience et ergonomie des systèmes déployés.

Ainsi, le système de téléphonie fixe OSIRIS déployé en 2017 enregistre désormais près de 100 heures d'appel par mois. Le système de visioconférence HORUS a quant à lui évolué pour s'appuyer sur le socle OSIRIS tout en améliorant l'expérience utilisateur. En matière de téléphonie mobile, SECDROID poursuit son développement avec plus de 20 000 téléphones acquis par la gendarmerie nationale au cours de l'année.

Bonnes pratiques appliquées aux autorités politiques

Au quotidien comme à l'approche de grands rendez-vous porteurs de risques (élections, sommets, compétitions sportives, etc.), l'ANSSI accompagne les ministères et hautes autorités dans la mise en œuvre de mesures de sécurité. Parce que les enjeux de sécurité numérique sont par nature complexes, l'agence fonde son approche sur la transmission et la bonne compréhension de ces enjeux. L'ANSSI est désormais attendue pour son rôle de conseil auprès de ce public. Ainsi, l'agence a engagé diverses initiatives à leur égard sous forme d'interventions ou de ressources documentaires.

RENCONTRE AVEC FLORIAN BACHELIER

PREMIER QUESTEUR DE L'ASSEMBLÉE NATIONALE, DÉPUTÉ D'ILLE-ET-VILAINE

FLORIAN BACHELIER

Vous rappelez régulièrement l'importance de sensibiliser et former à la sécurité numérique. De quelle manière cela se traduit-il au sein de l'Assemblée nationale ?

▼ Cela se traduit de trois façons différentes et complémentaires : assumer un renversement de doctrine en collaborant désormais avec l'ANSSI sur la protection cyber de l'Institution ; sensibiliser en continu les usagers du numérique que sont les équipes de l'Assemblée nationale (députés, fonctionnaires et collaborateurs) ; sensibiliser tous les députés à la dimension de gestion de risques cyber présente dans toutes les politiques publiques : de la santé à l'éducation en passant par la défense, les transports, les données personnelles, la presse, l'économie, etc.

Enfin, la mise en place du moteur de recherche français Qwant dans l'hémicycle est aussi un signal fort sur la maîtrise de la donnée numérique et l'enjeu de souveraineté que cela représente.

Vous êtes à la tête du groupe d'études sur la sécurité et la souveraineté numérique à l'Assemblée nationale : quels sont vos objectifs ?

▼ Le numérique, ça n'est pas un domaine d'activité, c'est une nouvelle forme d'organisation sociale, c'est le nouveau contrat social. Et le cyber en constitue l'avenant essentiel, vital.

La bataille de la donnée numérique constitue un enjeu absolu de souveraineté française et européenne puisqu'il innerve l'ensemble des politiques publiques de façon totalement transversale – de l'hygiène à la résilience, de l'éducation à la régulation, du défensif à l'offensif – et qu'il marque l'urgence du retour au projet politique européen qui est celui de la coopération entre États souverains.

Il nous faut sortir collectivement d'une forme de naïveté sur ces sujets et partir du réel, c'est-à-dire une bataille numérique mondiale incessante entre grandes puissances étatiques et privées. C'est également une formidable opportunité de création d'emplois. La France et l'Europe doivent prendre la place de chef de file dans ce combat mondial.

Selon vous, dans quelle mesure les députés peuvent-ils participer au développement de la confiance dans le cyberespace ?

▼ Les députés peuvent participer au développement de la confiance dans le cyberespace en organisant le cadre qui permet cette confiance.

L'espace numérique ne peut pas, ne peut plus, ne doit pas, ne doit plus échapper au droit. La France doit, en cette matière également, être aux avant-postes car nous ne croyons, ni ne voulons que le seul droit en vigueur dans le cyberespace soit en réalité les conditions générales d'utilisation des GAFAM.

La volonté politique est là. Il n'y a ni place, ni temps pour l'ignorance, la passivité ou la naïveté. Il nous faut être offensifs en intégrant que le cœur battant de cette stratégie, c'est l'école et c'est la formation.

DIFFUSER UNE CULTURE DE LA SÉCURITÉ NUMÉRIQUE

Gestion du risque numérique : une doctrine à la mesure des enjeux

La pleine implication des spécialistes du management du risque et des décideurs ne peut se faire sans l'accompagnement et les outils adéquats. C'est pourquoi la publication de la méthode d'analyse de risques EBIOS Risk Manager (cf. p. 9) est accompagnée de tout un arsenal méthodologique. Pour s'adresser à des publics non experts de la sécurité numérique, l'ANSSI mobilise les ressources et tisse les partenariats adéquats pour intégrer le risque numérique dans la prise en compte globale des risques.

« La gestion du risque numérique n'est pas seulement technique. Elle suppose l'implication de tous les échelons de l'organisation, de la direction aux équipes. »

Fabien Caparros,
chef de division management
de la sécurité numérique,
sous-direction stratégie

Ainsi, un supplément est venu compléter le guide EBIOS Risk Manager pour enrichir la méthode d'une palette d'outils facilitant l'appropriation et la mise en œuvre de celle-ci. À terme, le label éponyme renforcera encore la méthode avec la mise à disposition d'outils logiciels permettant la réalisation d'analyses de risques complètes.

Pour compléter ce corpus documentaire déjà doté de ressources utiles aux démarches d'homologation de sécurité, l'ANSSI fournit désormais une méthode d'aide à la réalisation d'une cartographie des systèmes d'information. Cette mesure d'hygiène informatique fondamentale et obligatoire pour les OIV s'intègre dans une démarche globale de gestion des risques. Utile à toute organisation quelles que soient sa nature, sa taille, sa maturité ou la complexité de son système d'information, le guide *Cartographie du système d'information* présente une démarche adaptée aux besoins opérationnels de ceux qui la mettent en œuvre.

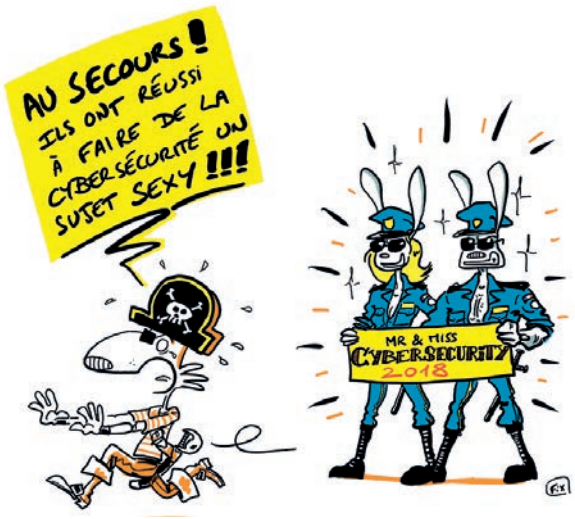
Enfin et toujours dans le souci de répondre aux préoccupations des décideurs, l'ANSSI et la DINSIC ont publié la méthode *Agilité et sécurité numériques* qui concilie habilement ces deux principes, exemples et expériences à l'appui.

Mois européen de la cybersécurité : la France innove et enthousiasme

Forts du succès de l'édition 2017, l'ANSSI et plus d'une trentaine de partenaires institutionnels (ministères, associations et fédérations, CCI, etc.) se sont à nouveau mobilisés en octobre pour faire du mois européen de la cybersécurité un temps fort qui éveille les consciences et l'intérêt autour des enjeux de sécurité numérique. Au rythme des événements organisés partout en France, de nouvelles initiatives ont marqué les esprits par leur originalité et leur capacité à rassembler toute une communauté d'acteurs.

Une campagne dessinée haute en couleurs

En faisant appel au dessinateur Fix, l'agence a misé sur l'humour et l'anecdote pour croquer la cybersécurité. À travers une quinzaine de dessins interpellant sur les risques liés à la sécurité des données, aux nouveaux usages ou encore à l'imaginaire collectif, l'ANSSI promeut les bonnes pratiques à mettre en œuvre sans plus attendre.



Challenge européen : une première participation remarquée

Autre nouveauté et véritable succès, la France a remporté pour sa première participation la deuxième place de l'*European Cybersecurity Challenge* (ECSC) ! Cette compétition européenne s'est tenue du 14 au 17 octobre 2018 et a opposé 17 équipes nationales composées de jeunes hackers éthiques âgés de 14 à 25 ans. En lien avec l'association HZN, l'ANSSI a activement participé à la sélection et à l'entraînement de l'équipe pour l'emmener en finale.

Faire face aux enjeux de demain

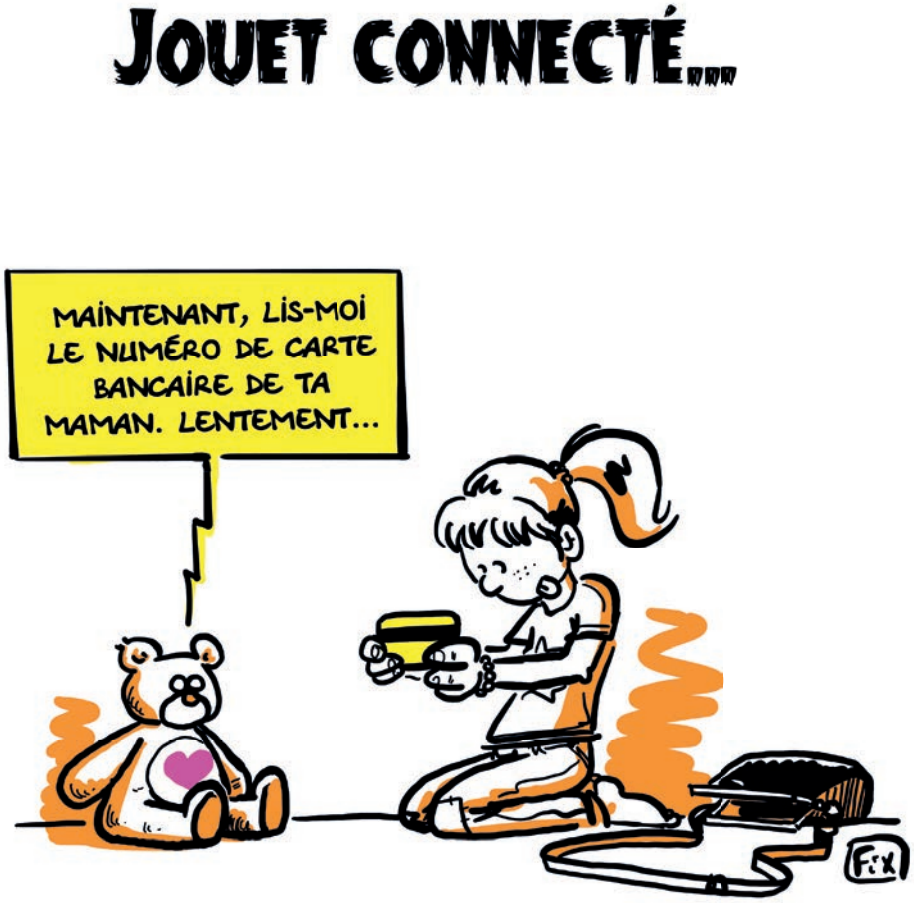
Parmi les sujets explorés lors du mois européen de la cybersécurité, les enjeux liés à l'Internet des objets (*Internet of Things* - IoT) ou encore à l'intelligence artificielle ont donné lieu à plusieurs initiatives. Ainsi, des événements dédiés à ces questions se sont tenus et la cour d'Appel de Paris s'est emparée du sujet en organisant à l'occasion de la Nuit du droit un procès fictif mettant en scène un immense carambolage de voitures autonomes dans les rues de Paris.

VOUS AVEZ DIT SYSTÈMES « CYBER-PHYSIQUES » ?

Si le concept ne vous dit rien, vous en avez certainement déjà croisés. On appelle systèmes « cyber-physiques » les systèmes qui créent une convergence entre les mondes physique et immatériel. De nombreux pans de l'économie (industrie, transports, santé, etc.) et de nos sociétés recourent désormais à ces technologies devenues, dans certains cas, indispensables.

L'une des premières conséquences de l'apparition massive des objets connectés est leur propension à accroître très fortement la surface d'exposition aux attaques. Celles-ci peuvent être dirigées vers l'objet lui-même, quand il ne s'agit pas tout bonnement d'en détourner la finalité pour les transformer en vecteurs d'actions malveillantes. Bien que très développé, le domaine des objets connectés est encore jeune et souffre d'un manque de maturité qui se traduit par une insuffisance de normes et l'absence de sécurité *by design*.

Si l'application de bonnes pratiques et de principes de sécurité tout au long du cycle de développement de ces systèmes participe à réduire les risques, cela ne suffira pas à protéger les environnements les plus sensibles tels que les systèmes industriels. De plus, les enjeux liés à la disponibilité de ses systèmes priment souvent sur la confidentialité ou l'authenticité. Cet aspect induit un changement de paradigme générateur de véritables défis techniques.



3 CONSERVER UN TEMPS D'AVANCE

L'EXPÉRIENCE ET L'EXPERTISE DE L'ANSSI LUI PERMETTENT DE MOBILISER SON ÉCOSYSTÈME, DE SE POSITIONNER ET DE SE PROJETER. CEPENDANT, POUR AVOIR DU SENS ET CRÉER DE L'ADHÉSION, IL EST ESSENTIEL QUE LES PROPOSITIONS QUE FORMULE L'AGENCE REÇOIVENT L'AVIS D'UNE LARGE COMMUNAUTÉ D'ACTEURS.

01 // L'OUVERTURE ET LE PARTAGE POUR MOTS D'ORDRE

De plus en plus, l'ANSSI confronte ses productions à l'appréciation de ses publics. En rejoignant des espaces de dialogue et en en créant d'autres, l'agence invite à la transmission de compétences et de connaissances.

OPEN SOURCE : UN ACTE DE TRANSPARENCE

L'ANSSI contribue à 13 projets Open Source. Une approche assumée et qui, au regard de récentes expériences, renforce l'ANSSI dans sa volonté de poursuivre dans cette voie.

CLIP OS : une histoire de patience et de confiance

L'ANSSI développe, fait évoluer et utilise CLIP OS depuis 2006. Basé sur Linux, ce système d'exploitation intègre un ensemble de mécanismes de sécurité qui lui confèrent un haut niveau de résistance aux codes malveillants et lui permettent d'assurer la protection d'informations sensibles.

Il fournit par ailleurs des mécanismes de cloisonnement qui rendent possible le traitement simultané, sur le même poste informatique, d'informations publiques d'une part et classifiées d'autre part, grâce à deux environnements logiciels isolés. L'objectif est ainsi de réduire les risques de fuite d'informations sensibles sur un réseau public.

S'il n'existe actuellement pas de version « prête à l'emploi » de CLIP OS pour le grand public, l'ANSSI propose à chacun de contribuer au développement et au durcissement du système d'exploitation, pour mieux répondre aux usages et aux besoins spécifiques de chaque déploiement. À cette fin, l'agence met à disposition de la communauté :

- le code source et la documentation en français de la version 4 de CLIP OS pour initier et faciliter les développements futurs ;
- le code source et la documentation en anglais de la version 5 de CLIP OS en cours de développement.

«Nous sommes persuadés que l'État doit activement participer à l'Open Source. Ces projets et la communauté qui les anime ont un potentiel considérable.»
Yann Bonnet,
directeur de cabinet

L'ÉCLAIRAGE DE TIMOTHÉE RAVIER

CHEF DE LA CELLULE DE DÉVELOPPEMENT CLIP OS, SOUS-DIRECTION EXPERTISE

TIMOTHÉE RAVIER

L'ouverture de CLIP OS à tous les contributeurs : qui l'eût cru ?

▼ À l'époque, on n'y croyait pas non plus. Nous sommes vraiment passés de l'idée à la mise en œuvre concrète en avril 2017. Dès lors, nous avons dû passer par une série d'étapes puisqu'il nous a d'abord fallu obtenir une version nettoyée de tout élément classifié avant d'envisager la publication en Open Source. Ce fut chose faite avec la sortie de la version 4, suivie de près par la version 5 entièrement conçue sur une base Open Source.

Quelles ont été les réactions de la communauté Open Source à l'annonce de la sortie de CLIP OS ? Et celles de tes collègues de l'ANSSI ?

▼ La sortie de CLIP OS en septembre 2018 a suscité pas mal de réactions, parmi lesquelles quelques retombées presse. Mais je retiens tout particulièrement le *Paris Open Source Summit* de décembre qui nous a permis d'échanger directement avec des membres de la communauté très attentifs au développement de telles initiatives. En interne aussi, la participation de l'agence à la communauté Open Source est de plus en plus visible. S'il ne s'agit pas de quelque chose de nouveau en soi, il nous est désormais plus facile de communiquer sur ces projets car l'on croit fermement en leur capacité à diffuser une culture de la sécurité numérique.

La saga dure depuis plus d'une décennie : CLIP OS nous réserve-t-il de nouvelles surprises ?

▼ Après la sortie de la version alpha du système en septembre, nous travaillons désormais à une version bêta disposant des briques de base indispensables à un déploiement à plus grande échelle (mise à jour système, communications sécurisées, chiffrement des données, etc.). À terme, l'objectif est de faire certifier la solution pour garantir – de manière indépendante de l'agence – que l'on applique les principes de sécurité que l'on édicte.

WooKey : la sécurité n'attend pas

Prototype de clé USB sécurisée appliquant plusieurs principes de sécurité essentiels, WooKey, c'est aussi une philosophie. En apportant aux fabricants la preuve par l'exemple qu'il est possible, pour un coût raisonnable, de conjuguer expérience utilisateur et sécurité, l'équipe projet encourage de manière concrète à intégrer la sécurité dès la conception.

Les raisons qui ont motivé ce projet puisent leurs racines dans la découverte de vulnérabilités touchant les périphériques USB. Les six membres de l'équipe ont donc concentré leurs efforts sur l'intégration de principes de sécurité dès la conception du périphérique. C'est ainsi que sur une clé USB dotée d'importantes capacités de stockage ont été appliqués les principes de défense en profondeur, l'authentification forte de l'utilisateur et le chiffrement des données.

Avec l'objectif de faire profiter au plus grand nombre d'une solution sécurisée clé en main, le schéma de la carte électronique ainsi que le code source du micro logiciel exécuté sont disponibles sur le GitHub de l'ANSSI.

Évaluer le niveau de sécurité de son Active Directory

Depuis la création de l'ANSSI, les prestations d'audit effectuées par l'agence auprès de ses bénéficiaires font apparaître un manque de maturité critique récurrent sur la sécurité des annuaires Active Directory (AD), point névralgique dans les systèmes d'information Windows. Ce défaut de sécurité affaiblit significativement le niveau global de sécurité de ces SI. Cette observation est également confortée par la connaissance obtenue au contact des différents réseaux compromis sur lesquels l'ANSSI est intervenue lors d'opérations de cyberdéfense. Au-delà de ce manque de maturité, le bureau audits constate par ailleurs que le niveau de sécurité des annuaires AD décroît en fonction du temps et de la vie du SI.

Face à ce constat, le bureau a développé un nouveau service dont l'objectif est d'auditer régulièrement, à la demande et de manière autonome, le niveau de sécurité des AD des ministères. Les résultats sont mis à disposition du souscripteur du service sous la forme d'une interface Web qui répertorie de façon ordonnée les vulnérabilités et recommandations afférentes. Lors de chaque audit fait à la demande, une indication globale du niveau de sécurité de la configuration de l'AD est émise sur une échelle de 1 à 5. Le niveau obtenu découle immédiatement de la gravité des vulnérabilités trouvées. Un niveau donne ainsi accès à un lot de recommandations adaptées.

L'application de l'ensemble des recommandations portant sur les points importants d'un niveau permet de passer au niveau supérieur et par conséquent d'avoir accès à une collection complémentaire de recommandations. Considérant l'enjeu majeur pour un réseau qu'est la bonne sécurisation de son AD (et son maintien), l'objectif du service est d'accompagner progressivement ses bénéficiaires vers un niveau de sécurité à l'état de l'art. Dans une démarche de transparence, l'agence a opté pour la publication du code source de l'outil de collecte sur GitHub (outil ORADAD). Ce nouveau service est développé en amélioration continue et bénéficie au quotidien des retours et commentaires de ses utilisateurs finaux.

ESPACES DE RÉFLEXION

L'ANSSI communique et s'ouvre chaque jour davantage. C'est pourquoi elle s'exprime dans un souci permanent de clarté et d'objectivité. Pour tendre vers cet objectif, l'agence renforce ses liens avec d'autres acteurs et en crée de nouveaux dans le but de mobiliser un écosystème favorable à la réalisation de certains projets impliquant le monde académique, l'entreprise, l'éducation ou encore la société civile.

Agora 41 : s'extraire des codes

L'ANSSI a lancé en septembre 2018 l'Agora 41. Originale, libre et dynamique, cette assemblée a vocation à engager et nourrir une réflexion globale sur des sujets non techniques mais en prise directe avec les enjeux de sécurité numérique que l'agence doit relever. Les membres de l'Agora se réunissent ainsi régulièrement pour réfléchir collectivement et librement à des thèmes identifiés par l'agence (imaginaire collectif, talents, écosystème, etc.).

02 // ANTICIPER : UN PRÉREQUIS POUR L'AVENIR

Intelligence artificielle, santé connectée, informatique quantique… Comment sécuriser les technologies de demain ? Plus que jamais, il est essentiel de se réunir autour de ces problématiques qui amènent progressivement à changer de paradigme et envisager la façon dont l'ANSSI et son écosystème assureront leurs missions dans un futur proche.

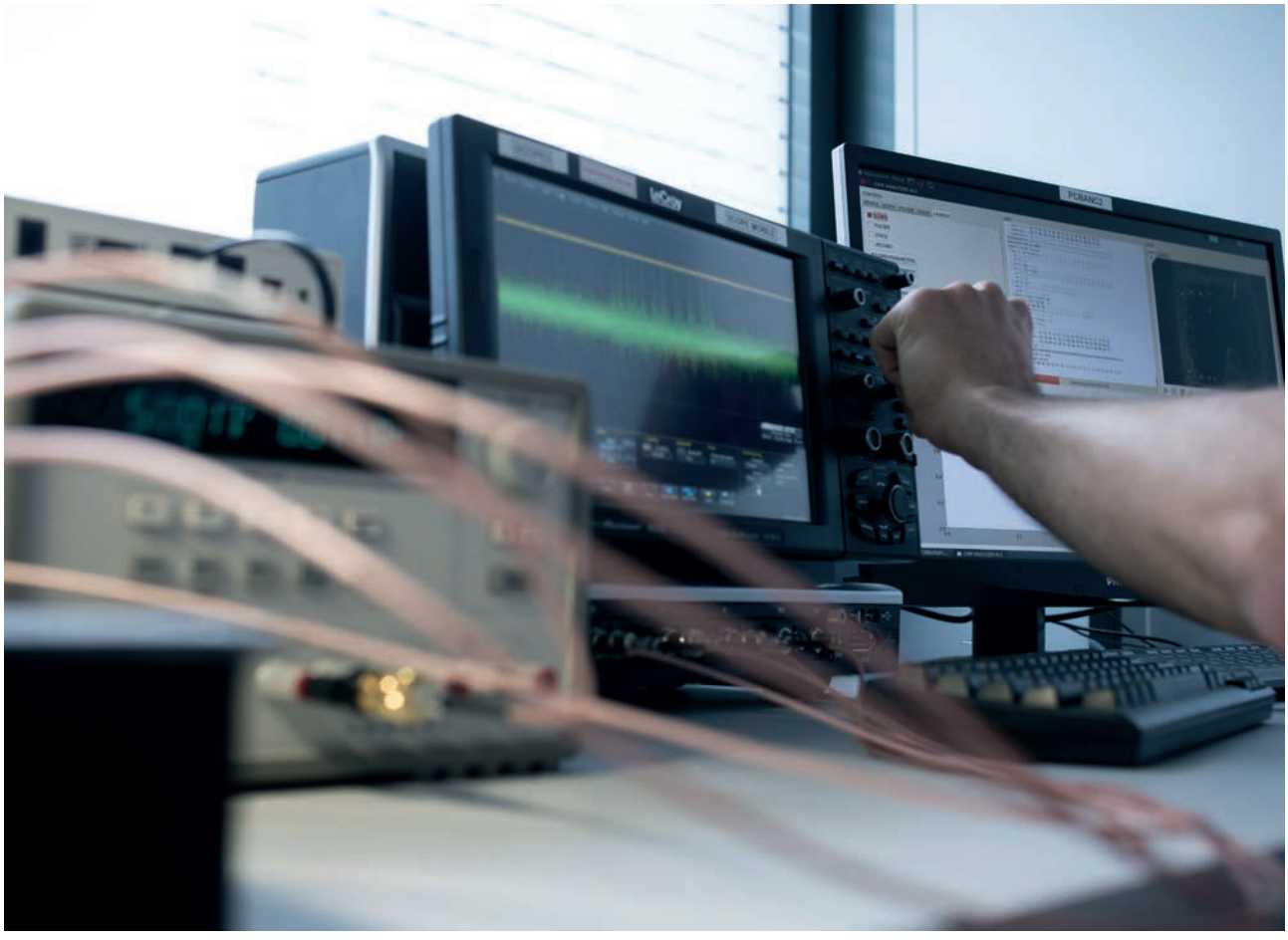
RECHERCHE : UNE ACTIVITÉ DYNAMIQUE ET RECONNUE

L'ADN de l'ANSSI demeure avant tout technique et scientifique. Pour preuve, l'activité de recherche entre dans une nouvelle dynamique et ajoute de nouvelles cartes à son jeu pour relever, aux côtés d'experts reconnus, les défis intellectuels que pose la sécurité numérique.

Conseil scientifique : un nouveau cadre d'échanges

Très à l'écoute de l'avis de ses pairs et soucieuse de recueillir leur soutien dans les projets qu'elle mène, la division scientifique et technique de l'ANSSI a constitué un conseil scientifique dont l'activité débutera en 2019. Pour l'agence, la formation de ce pôle d'experts vise à faciliter les interactions qui existent entre elle et le monde académique tout en orientant ses travaux de recherche en vue de rester à l'état de l'art.

Un rapport d'activité scientifique rappelant les projets menés par la division – en propre ou de manière collaborative – sera remis aux membres du conseil scientifique pour initier la démarche et recueillir leurs réactions.



RENCONTRE AVEC GILDAS AVOINE

PROFESSEUR EN SÉCURITÉ INFORMATIQUE ET CRYPTOGRAPHIE À L'INSA RENNES, PRÉSIDENT DU CONSEIL SCIENTIFIQUE

GILDAS AVOINE

Au cœur de l'écosystème de recherche national, quels liens entretenez-vous avec l'ANSSI ?

▼ L'écosystème national est riche et diversifié ; il se structure autour de chercheurs issus de grands centres de recherche et d'enseignants-chercheurs des universités et écoles. Les uns et les autres se retrouvent parfois dans des laboratoires communs appelés Unités mixtes de recherche (UMR), une spécificité française. L'activité de recherche de l'agence est reconnue par la communauté scientifique. La participation d'agents de l'ANSSI aux conférences et leurs publications nous donnent l'occasion de nous rencontrer régulièrement. La nature et la qualité de ces liens ont amené l'ANSSI à me proposer d'assurer la présidence de son conseil scientifique. L'objectif est précisément de conseiller l'agence sur les thématiques de recherche à privilégier, les conférences auxquelles participer, etc. dans le but d'orienter et répartir au mieux les efforts et les ressources.

Selon vous, quelles tendances préfigurent les grands défis que les experts de la sécurité numérique auront à relever au cours des prochaines années ?

▼ Je dirige le groupement de recherche en sécurité informatique du CNRS qui rassemble près de 1 000 chercheurs. Dans ce cadre, nous nous sommes posé cette question et avons identifié un certain nombre de défis majeurs. J'en évoquerai cinq pour illustrer ce travail. Le premier concerne la cryptographie post-quantique. Ce sujet d'actualité mobilise des chercheurs du monde entier dans l'objectif de trouver des algorithmes capables de résister à la puissance d'un ordinateur quantique. Le second défi porte sur la cryptographie homomorphe. Cette dernière doit permettre la réalisation de calculs sur des données chiffrées, une solution particulièrement intéressante à l'heure du Cloud pour déléguer des calculs sans révéler les données. Le troisième concerne les preuves, c'est-à-dire qu'il consiste à prouver, sous certaines hypothèses, qu'un système est sûr. Le quatrième défi concerne l'intelligence artificielle et les perspectives qu'elle pourrait offrir en matière de cybersécurité. Le cinquième et dernier défi est quant à lui proche des sciences humaines puisqu'il s'intéresse à la vie privée et à l'éthique pour s'interroger, par exemple, sur la pertinence d'être transparent ou non sur les algorithmes utilisés.

La sécurité numérique repose sur la responsabilité partagée d'un nombre croissant d'acteurs. Dans ce contexte, de quelle manière les chercheurs participent-ils à relever ces défis ?

▼ Les chercheurs participent au défi de la sécurité numérique en apportant des solutions à de nouveaux besoins ou en formant professionnels et citoyens. On assiste ainsi à une forme de transfert de compétences et de connaissances entre différents mondes. Il arrive également que le monde académique exerce une forme de contre-pouvoir à l'égard de certains intérêts économiques en soulignant un défaut de sécurité. Il encourage ainsi une prise de responsabilité partagée.

INTELLIGENCE ARTIFICIELLE : DES ENJEUX BIEN RÉELS

L'intelligence artificielle (IA) se donne comme objectif de doter un système de la faculté d'apprendre par lui-même des tâches complexes et potentiellement difficiles à programmer. Le champ des possibles est gigantesque et touchera tous les domaines des activités humaines et techniques allant du transport autonome jusqu'aux interactions « en langage naturel » avec des outils technologiques.

Par sa capacité inédite de traitement d'énormes volumes de données, l'IA va bouleverser des secteurs entiers de l'économie. Même si les limites et les capacités de cette technologie sont encore imprécises et non maîtrisées, il est d'ores et déjà possible d'envisager certains risques (apparition de nouvelles vulnérabilités, utilisation de l'IA des fins malveillantes) et opportunités (aide à la détection des attaques informatiques) du point de vue de la sécurité des systèmes d'information et du cyberespace en général. Enfin, si l'IA laisse entrevoir de nouvelles possibilités, se pose également la question de savoir comment évaluer cette technologie.

Au-delà des questions éthiques liées au développement de l'IA, la prise en compte de la sécurité dès la conception des nombreux projets ayant recours à ces nouvelles technologies apparait donc comme une condition sine qua non de son acceptation sociale.

Un groupe de travail stratégique pour anticiper les usages

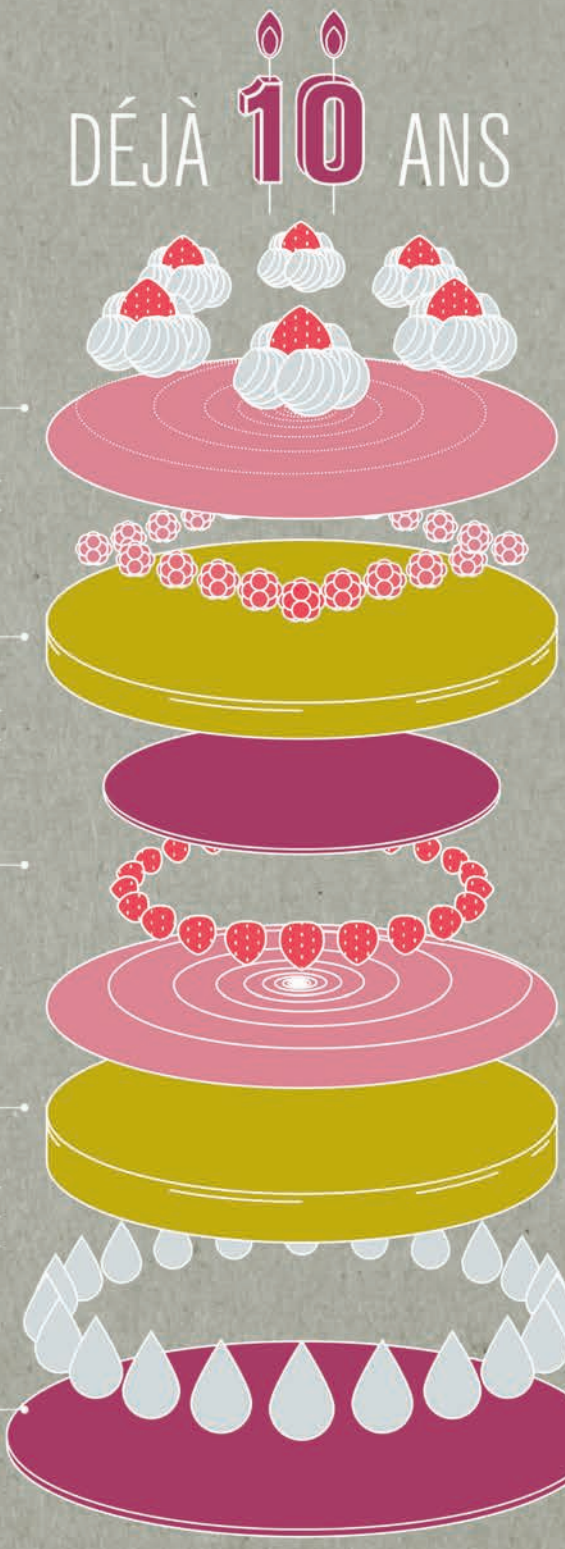
En 2018, un groupe de travail interne à l'ANSSI s'est réuni à plusieurs reprises pour identifier et comprendre les grandes tendances relatives aux usages émergents observés chez les acteurs que l'agence protège et défend. Plus spéculative que l'approche consistant à identifier les tendances technologiques, cette démarche a néanmoins permis d'aboutir à l'édiction de constats et de recommandations concrètes. Avec un regard dégagé sur les missions actuelles de l'agence, les membres du groupe de travail ont ainsi identifié des tendances qui viennent nourrir des travaux internes et accompagner la transformation de l'agence sur le long terme.

À l'origine de cette initiative, la pleine conscience de l'ANSSI de sa mission de vigie technologique. Cette dernière consiste non seulement à anticiper les ruptures technologiques et évolutions des usages mais aussi à en identifier suffisamment tôt l'émergence pour pouvoir les accompagner efficacement. Sans cela et si l'agence ne se donne pas les moyens – et le temps – de le faire, comment accompagner efficacement les bénéficiaires ; entrainer autour d'elle et avec elle ; orienter ses travaux de recherches ; faire entendre sa voix en Europe et à l'international ; se structurer et former ses agents ; nouer les bons partenariats ?

Les interrogations que soulève le rapport issu de ces réflexions méritent que l'ANSSI n'y réfléchisse pas seule.

C'est la raison pour laquelle les travaux du groupe de travail ont vocation à dépasser les frontières de l'agence pour être commentés et enrichis par d'autres. Le présent rapport annuel – en abordant la perte de notion de périmètre du système d'information, les systèmes cyber-physiques et l'intelligence artificielle – constitue un premier pas en ce sens.

DÉJÀ 10 ANS



2018

UNE ANNÉE STRATÉGIQUE POUR LA FRANCE

L'ANSSI pilote la transposition de la directive NIS en France et déploie sa doctrine de management du risque.

2017

PREMIÈRE CONFÉRENCE SUR LA PAIX ET LA SÉCURITÉ DANS LE CYBERESPACE

Un débat nécessairement international initié par la France.

2016

ADOPTION PAR L'EUROPE DE LA DIRECTIVE NIS

Un modèle français qui inspire.

2015

STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE

La consolidation d'une vision stratégique nationale pour la cyberdéfense.

2014

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ÉTAT

Des règles de protection des systèmes sont fixées pour les départements ministériels.

2013

L'ANSSI AUX CÔTÉS DES OPÉRATEURS D'IMPORTANCE VITALE

Légiférer pour élever le niveau de cybersécurité des infrastructures critiques.

2012

UN RAPPORT EN FAVEUR DU RENFORCEMENT DES MOYENS DE L'ANSSI

Anticiper pour mieux répondre aux enjeux de cyberdéfense.

2011

L'ANSSI DEVIENT L'AUTORITÉ NATIONALE DE DÉFENSE DES SYSTÈMES D'INFORMATION

Émergence d'un modèle français de cyberdéfense.

2010

L'ANSSI DÉVELOPPE UNE CAPACITÉ CENTRALISÉE DE DÉTECTION

Prévenir les attaques ciblant les systèmes d'information de l'État.

2009

CRÉATION DE L'ANSSI

L'État se dote d'une capacité de prévention face aux attaques informatiques.

10 ANS / 10 TEMPS FORTS

En 10 années, beaucoup de choses ont changé : structure, missions, rayonnement... Et pourtant, l'essentiel est toujours là : un modèle capable d'accueillir toutes ces transformations, une expertise qui fait notre ADN et, surtout, un état d'esprit.

BIBLIOGRAPHIE

DOCUMENTS DE DOCTRINE

// MISES À JOUR

▷ *Recommandations relatives à l'administration sécurisée des systèmes d'information,* guide technique
Recommendations to secure administration of IT systems, technical guide

// NOUVEAUX

▷ *Recommandations pour choisir des pare-feu maîtrisés dans les zones exposées à Internet,* guide technique

▷ *Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux,* guide technique

▷ *Recommandations sur le nomadisme numérique,* guide technique

▷ *Cartographie du système d'information – Guide d'élaboration en 5 étapes,* guide méthodologique

▷ *EBIOS Risk Manager,* guide méthodologique

▷ *Protection du potentiel scientifique et technique de la nation,* guide méthodologique

▷ *Dispositifs réglementaires de sécurité du SGDSN – Analyse des trois dispositifs de protection nationaux (PSDN, SAIV, PPST),* plaquette

// APPELS À COMMENTAIRES

▷ *Bonnes pratiques de sécurité numérique à l'usage des professionnels en déplacement, mise à jour du Passeport de conseils aux voyageurs,* guide

▷ *Sécurité du numérique des collectivités territoriales : l'essentiel de la réglementation,* guide

▷ *Référentiel d'exigences de sécurité pour les moyens d'identification électronique,* référentiel

PUBLICATIONS INTERNES

▷ *Les valeurs de l'ANSSI,* livret

// CATALOGUE DES PRODUCTIONS DE L'ANSSI

▷ Actualité cyber

▷ Séminaire *Hack me if you can*

▷ EBIOS Risk Manager

▷ CLIP OS

▷ Valorisation des productions de l'ANSSI

// .ZIP, MAGAZINE INTERNE

▷ N°6 du 12 mars 2018

▷ N°7 du 23 juillet 2018

PUBLICATIONS SCIENTIFIQUES

// BUREAU AUDIT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

▷ Matthieu Buffet, Julien Raeis : *Audit de sécurité d'un environnement Docker* – SSTIC 2018, Rennes, France

▷ Jean-Baptiste Galet : *Machines virtuelles protégées* – SSTIC 2018, Rennes, France

// BUREAU DÉVELOPPEMENT DE DISPOSITIFS DE DÉTECTION

▷ Matthieu Treussart : *ProbeManager : Outil centralisé de gestion de sondes IDS* – SSTIC 2018, Rennes, France

// LABORATOIRE ARCHITECTURE MATÉRIELLE ET LOGICIELLE

▷ Mickaël Salaün : *File access-control per container with Landlock* – FOSDEM

▷ Ryad Benadjila, Arnauld Michelizza, Mathieu Renard, Philippe Thierry, Philippe Trebuchet : *WooKey: USB devices strike back* – SSTIC, Rennes, France

▷ Ryad Benadjila, Arnauld Michelizza, Mathieu Renard, Philippe Thierry, Philippe Trebuchet : *WooKey: the USB battlefront warrior* – Embedded Recipes

▷ Yves-Alexis Perez : *Dans les coulisses de l'équipe sécurité Debian* – SSTIC 2018, Rennes, France

▷ Mickaël Salaün : *Internal of Landlock: a new kind of Linux Security Module leveraging eBPF* – Pass the SALT

▷ Yves-Alexis Perez : *Debian security team: behind the curtains* – Pass the SALT

▷ Mickaël Salaün : *How to safely restrict access to files in a programmatic way with Landlock* – Linux Security Summit North America

▷ Thomas Letan, Yann Régis-Gianas, Pierre Chifflier, Guillaume Hiet : *Modular Verification of Programs with Effects and Effect Handlers in Coq* – Formal Methods

▷ Timothée Ravier, Mickaël Salaün : *CLIP OS: building a defense-in-depth OS around Linux kernel* – Kernel Recipes

▷ Timothée Ravier : *Clip OS : un système d'exploitation durci utilisant le noyau Linux et un environnement de logiciels Open Source* – Paris Open Source Summit

▷ Yves-Alexis Perez : *Linux kernel security contributions by ANSSI* – Linux Security Summit Europe

▷ Arnaud Michelizza : *Secure embedded system design: Introducing EwoK, an Open Source Ada microkernel* – High Integrity Software

// LABORATOIRE CRYPTOLOGIE

▷ L. Barthelemy, D. Kahrobaei, Guénaël Renault, Z. Sunic : *Quadratic Time Algorithm for Inversion of Binary Permutation Polynomial* – ICMS 2018, 19-27.

▷ C. Boura, A. Canteaut, Jérémy Jean, V. Suder : *Two Notions of Differential Equivalence on Sboxes* – Designs, Codes and Cryptography, Springer 2018, pp. 1-18.

▷ C. Chaigneau, Thomas Fuhr, Henri Gilbert, Jian Guo, Jérémy Jean, Jean-René Reinhard, Ling Song : *Key-Recovery on Full Kravatte: Transactions on Symmetric Cryptography 2018, vol. 1, IACR 2017.* (best paper award) – FSE 2018

▷ B. Cogliati, Yannick Seurin : *Analysis of the single-permutation encrypted Davies-Meyer construction* – Designs, Codes and Cryptography, Springer 2018

▷ P. Derbez, P.-A. Fouque, Jérémy Jean, B. Lambin : *Variants of the AES Key Schedule for Better Truncated Differential Bounds* – SAC 2018, LNCS, Springer 2018

▷ Thomas Fuhr, M. Naya-Plasencia, Y. Rotella : *State recovery attacks on modified Ketje Jr.* – FSE 2018, Transactions on Symmetric Cryptography 2018, vol. 1, IACR 2018

▷ F, Morain, Guénaël Renault, B. Smith : *Deterministic Factoring with Oracles* – CoRR abs/1802.08444

// LABORATOIRE EXPLORATION ET RECHERCHE EN DÉTECTION

▷ Anaël Beaugnon, Francis Bach, Pierre Chifflier : *End-to-End Active Learning for Computer Security Experts* – AICS 2018

▷ Anaël Beaugnon : *Expert-in-the-Loop Supervised Learning for Computer Security Detection Systems* – Thèse de doctorat 2018

▷ Anaël Beaugnon, Francis Bach, Pierre Chifflier : *End-to-End Active Learning for Computer Security Experts (version étendue de AICS)* – IDEA 2018

▷ Emmanuel Prouff, Rémi Strullu, Ryad Benadjila, Eleonora Cagli, Cécile Dumas : *Study of Deep Learning Techniques for Side-Channel Analysis and Introduction to ASCAD Database* – IACR 2018

▷ Anaël Beaugnon : *Machine Learning for Computer Security Detection Systems: Practical Feedback and Solutions* – C&ESAR 2018

// APPEL À COMMENTAIRES

▷ Pierre Chifflier : *Recommandation pour le développement sécurisé avec le langage de programmation Rust* – GitHub

// LABORATOIRE RÉSEAU, PROTOCOLES ET PREUVES

▷ Sébastien Mainand : *BUS CAN – Se lancer dans l'analyse des communications de votre véhicule* – Magazine MISC

// LABORATOIRE SÉCURITÉ DES COMPOSANTS

▷ Guillaume Bouffard, Léo Gaspard : *Hardening a Java Card Virtual Machine Implementation with the MPU* – SSTIC 2018

▷ Emmanuel Prouff, Houssem Maghrebi : *On the Use of Independent Component Analysis to Denoise Side-Channel Measurements* – COSADE 2018

▷ Emmanuel Prouff, Hervé Chabanne, Houssem Maghrebi : *Linear Repairing Codes and Side-Channel Attacks* – TCHES 2018

▷ Louiza Khati, Damien Vergnaud : *Analysis and Improvement of an Authentication Scheme in Incremental Cryptography* – SAC 2018

▷ Pooya Farshim, Louiza Khati, Damien Vergnaud : *Security of the Even-Mansour Ciphers under Key-Dependant Message* – IACR 2018

// LABORATOIRE SANS-FIL

▷ José Lopes-Esteves, Emmanuel Cottais, Chaouki Kasmi : *Détection de Diaphonie et AGREMI par une approche SSI* – CEM France 2018, Paris, France

▷ José Lopes-Esteves, Emmanuel Cottais, Chaouki Kasmi : *Software Instrumentation of an UAV for HPEM Effects Detection* – URSI AT-RASC, Gran Canaria, Espagne

▷ José Lopes-Esteves, Emmanuel Cottais, Chaouki Kasmi : *Second Order Soft Tempest in RF Front-ends: Design and Detection of Polyglot Modulations* – EMC Europe 2018, Amsterdam, Hollande

▷ José Lopes-Esteves, Emmanuel Cottais, Chaouki Kasmi : *Unlocking the Access to the Effects induced by IEMI on a Civilian UAV* – EMC Europe 2018, Amsterdam, Hollande

▷ Valentin Houchouas, Emmanuel Cottais, Marc Hélier, Muriel Darces, Nicolas Bourey, Yves Chatelon : *Comparison between simulation and measurement of EMI inside a computer chassis mock-up* – EMC Europe 2018, Amsterdam, Hollande

▷ Tristan Claverie, José Lopes-Esteves, Chaouki Kasmi : *SmartTVs: Security of DVB-T* – SSTIC 2018, Rennes, France

▷ Benoit Michau : *Pycrate : tester les systèmes télécoms et cellulaires avec Python* – SSTIC 2018, Rennes, France

▷ Pierre-Michel Ricordel, Emmanuel Duponchelle : *Risques associés aux signaux parasites compromettants : le cas des câbles DVI et HDMI* – SSTIC 2018, Rennes, France

▷ José Lopes-Esteves, Emmanuel Cottais, Chaouki Kasmi : *Software Instrumentation of an UAV for HPEM Effects Detection* – AMEREM, Santa Barbara, USA

▷ José Lopes-Esteves, Emmanuel Cottais, Chaouki Kasmi : *Remote Detection of HPEM attacks on Wireless Front-Ends* – AMEREM, Santa Barbara, USA

▷ José Lopes-Esteves, Emmanuel Cottais, Chaouki Kasmi : *Strategies to harden and neutralize UAV using RF DEW* – Hardwear.io, La Haye, Hollande

▷ Benoit Michau : *La sécurité des modems et terminaux mobiles* – Journées pré-GDR 2018 (CNRS), Paris, France

▷ José Lopes-Esteves, Chaouki Kasmi : *Remote and Silent Voice Command Injection on a Smartphone through Conducted IEMI: Threats of Smart IEMI for Information Security* – Journal, System Design and Assessment Notes, Summa Foundation

▷ Christophe Devine, Adrian Thillard, Manuel San Pedro : *A Practical Guide to Differential Power Analysis of USIM Cards* – SSTIC 2018, Rennes, France

PUBLICATIONS TOUS PUBLICS

▷ *Rapport d'activité 2017 (FR + EN)*

▷ Plaquette institutionnelle

▷ *Rançongiciels : vos données sont prises en otage,* infographie

▷ *Hameçonnage : on vous incite à communiquer des informations,* infographie

PARTENARIATS

▷ ANSSI-DINSIC : *Agilité & sécurité numériques – Méthode et outils à l'usage des équipes projet,* guide méthodologique

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

51, BOULEVARD DE LA TOUR-MAUBOURG
75700 PARIS CEDEX 07 SP

COMMUNICATION@SSI.GOUV.FR
WWW.SSI.GOUV.FR

@ANSSI_FR
DAILYMOTION.COM/ANSSI_FR
LINKEDIN.COM/COMPANY/ANSSI-FR

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN