RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

La revue annuelle
de l'ANSSI
Édition 2020

Papiers numériques

La revue annuelle
de l'ANSSI
Édition 2020

Papiers numériques

Remerciements

À l'image de l'ANSSI, les *Papiers numériques* puisent leur identité et leur singularité dans l'influence réciproque qui s'exerce entre l'agence et ses partenaires. Pour être au plus près de ce qu'est l'ANSSI, un comité de rédaction composé de huit agents a accompagné la réalisation de la revue, de la définition des sujets à la validation des contenus en passant par la recherche documentaire. Un élan interne qui passe également par de nombreux partages d'expérience. Pour la qualité de leurs contributions, leur enthousiasme et leur disponibilité, nous remercions chaleureusement nos collègues pour leur participation à ce numéro !

Les *Papiers numériques* sont aussi un micro tendu vers nos partenaires car les enjeux de cybersécurité ne s'appréhendent correctement qu'à la lumière de plusieurs éclairages. Pour la richesse de notre collaboration, leur engagement et leur générosité, merci à toutes celles et ceux qui ont accepté de joindre leur voix à la nôtre pour ce numéro : Alice Chérif, Julien Chiaroni, Laurence Haguenauer, Claudie Haigneré, Hugo Horiot, William Lecat, Saâd Kadhi, David Pointcheval, Valérie Peneau, Bruno Sportisse, Michel Van Den Berghe, Henri Verdier et Patricia Zorko.

Vision(s)

Le positionnement interministériel de l'ANSSI auprès du SGDSN est au cœur du modèle français de cyberdéfense. À la tête des deux instances, Claire Landais et Guillaume Poupard nous offrent leur vision de l'agence.

CLAIRE LANDAIS
Secrétaire générale de la défense et de la sécurité nationale

GUILLAUME POUPARD
Directeur général de l'ANSSI

En 2019, l'ANSSI fêtait ses dix ans : ça vous inspire quoi ?

CLAIRE LANDAIS :
L'ANSSI est née d'une ambition: faire entrer la cybersécurité au cœur des enjeux de sécurité nationale. Depuis sa création et face à l'évolution de la menace, elle n'a jamais cessé d'innover et de convaincre pour assoir son rôle. Chaque brique posée a conduit l'ANSSI à ce qu'elle est aujourd'hui : l'actrice opérationnelle de référence, un pôle d'expertise reconnu et plus que jamais, une véritable animatrice de la communauté de la cybersécurité. Il faut dire qu'elle a été brillamment servie par des équipes remarquables et visionnaires, qui ont su la conduire dans la bonne direction.

GUILLAUME POUPARD :
Dix ans... que de changements en si peu de temps ! Évolution des usages, de la menace, de la prise en compte du risque, de nos capacités techniques et opérationnelles, etc. Dix ans pendant lesquels l'ANSSI a bâti avec ses nombreux partenaires un édifice robuste permettant de mieux prévenir le risque, de détecter les attaques, d'aider les victimes, de façonner les systèmes

les plus sensibles tout comme notre comportement quotidien pour une prise en compte au juste niveau de la sécurité numérique. Que de chemin parcouru… mais nous ne sommes qu'au début de l'aventure !

Est souvent rappelée l'importance de conserver l'âme de l'agence : mais comment la définiriez-vous ?

C.L. : Je constate, avec chaque interlocuteur, à quel point l'ANSSI rayonne. Reconnue, entendue, elle parvient à fédérer une impressionnante variété d'acteurs. Et à raison ! Si elle est écoutée, c'est qu'elle a su démontrer l'objectivité de son expertise technique. Je crois aussi que l'ANSSI constitue un exemple par son identité particulière, à la confluence de plusieurs cultures et de plusieurs générations. C'est aussi sans doute en partie ce qui fonde ses valeurs.

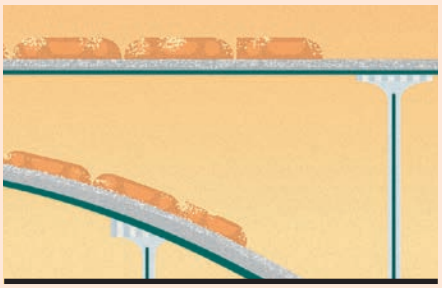
G.P. : L'agence est un OVNI administratif et c'est sa force. Nos autorités ont rendu possible la création d'une entité capable d'agir sur tous les fronts : réglementaire, technique, opérationnel, stratégique. Cette intégration de compétences variées et de haut niveau nous permet de développer une politique cohérente et efficace, au profit de nos bénéficiaires. Mais la croissance de l'agence ne doit pas faire disparaître l'esprit d'équipe, la cohésion, l'exigence permanente qui prévalent depuis l'origine. Nous résumons cela dans nos valeurs – ouverture, agilité, compétence – mais au-delà c'est un véritable esprit de corps qui lie l'ensemble des agents.

En quoi l'ANSSI et le SGDSN partagent-ils une culture commune ? Et des cultures distinctes ?

C.L. : Au sein d'une maison dont les efforts doivent souvent rester secrets, l'ANSSI doit former, informer, sensibiliser – finalement, être ouverte ! – pour assurer la sécurité des organisations essentielles et améliorer celle de l'ensemble de la société. C'est peut-être sa principale singularité. Mais notre point commun est de travailler sous l'autorité du Premier ministre, pour protéger nos concitoyens. 2020 sera l'occasion d'une évolution, puisque la sous-direction du Numérique de l'ANSSI et le Centre de transmissions gouvernemental du SGDSN s'allieront pour créer l'Opérateur des systèmes d'information interministériels classifiés (OSIIC). L'enjeu, c'est de renforcer les synergies et la lisibilité de nos actions. Ce sont deux belles équipes qui ont chacune une identité et un fonctionnement propres. Je sais qu'elles parviendront à construire ensemble l'entité qui répondra aux besoins croissants des autorités de l'État en termes de communications sécurisées.

G.P. : La raison d'être de l'ANSSI est la sécurité numérique de la nation, de nos concitoyens, de nos opérateurs d'importance vitale, mais également économiques et sociétaux. Son rattachement à la Secrétaire générale est donc une évidence et une force de notre modèle. Nous bénéficions ainsi d'une réelle proximité avec les plus hautes autorités de l'État et d'une prise en compte globale de l'ensemble des questions de sécurité. Qu'importent les différences de statuts, de parcours ou encore de tenues vestimentaires, les agents de l'ANSSI partagent avec le reste du SGDSN une même volonté de mise à disposition de leurs expertises au profit de l'intérêt général ! ●

Sommaire



Les données et connaissances issues des activités de cybersécurité sont d'une grande valeur. L'ANSSI a à cœur de les partager chaque fois que cela est possible pour, collectivement, les faire fructifier et élever le niveau global de sécurité.

Une vision partagée ; une ambition collective

Dix ans, déjà ! En 2019, plutôt que de se livrer à un exercice nostalgique, l'ANSSI a pris le parti de se projeter vers l'avenir. Dans un souci d'amélioration continue, elle a cherché à développer et à expérimenter de nouvelles pratiques, favorisant une ouverture et une mise en commun de plus en plus systématiques. Semant quelques graines, elle a au passage appelé ses partenaires à embrasser la même philosophie. Une invitation à s'engager, collectivement, pour la confiance numérique.

Il y a des évènements qui restent dans la mémoire des organisations. Pour l'ANSSI, le Cyber Festival est de ceux-là. Le 4 juin 2019, l'agence fêtait le dixième anniversaire de sa création. Et pour l'occasion, elle avait invité ses partenaires à partager un moment privilégié d'échange et de convivialité. De quoi faire fi de toute logique chronologique et entamer le récit de l'année par cet évènement printanier.

Fête de la « cyber »

Plusieurs espaces, plusieurs ambiances : ce jour-là, au Ground Control de Paris, ce qu'on aime appeler « l'écosystème » cyber a déambulé dans un lieu aménagé pour parler à toute sa diversité. Fourmillant dans le hangar, plus de 1 000 personnes ont notamment pu assister à de nombreuses tables rondes et présentations ou découvrir l'activité de spécialistes de la sécurité des systèmes d'information – tous métiers confondus.

Parce qu'un anniversaire est avant tout une fête, la journée fut aussi l'occasion de lâcher prise, ensemble, en participant à une fresque collaborative, en testant le studio radio ou en défiant ses collègues sur un terrain inédit: autour d'un flipper ou d'un jeu d'arcade. Pour les agents de l'ANSSI, point de mot d'ordre si ce n'est : *come as you are!*

Dans un joyeux brouhaha se croisaient ainsi, pêle-mêle, des élus et représentants du secteur public, des acteurs du monde de l'entreprise, des ingénieurs et informaticiens, des responsables de la sécurité informatique, des étudiants, des chercheurs ou encore des journalistes. Beaucoup d'hommes et, plus nombreuses que jamais, des femmes parvenues à dépasser les déterminismes sociaux pour rejoindre l'univers de « la cyber ».

En interne, la journée a souvent été vécue, si ce n'est comme un tournant, au moins comme un moment structurant. C'était d'abord un constat : après dix ans d'existence, l'agence a pu bâtir un socle suffisamment solide pour réunir autour d'elle une communauté enthousiaste à l'idée de relever collectivement le défi de la sécurité numérique.

Pourtant, au-delà du bilan, le Cyber Festival était surtout une occasion de regarder vers l'avenir. Et une opportunité pour l'agence, à travers la voix de son directeur général, de dessiner une trajectoire placée sous le signe de l'ouverture et de l'innovation.

« Symboliquement, cet évènement démontre que l'agence est prête à s'ouvrir et à partager. »

BAPTISTE SORIN
Chef adjoint de la division Communication

Devant l'assemblée, Guillaume Poupard l'a affirmé : « *C'était une journée à l'image de ce que je souhaite que l'agence soit* ». Original, le format de l'évènement était presque une preuve de concept. C'était en tout cas un moment tout choisi pour annoncer trois pistes stratégiques, pour l'agence comme pour l'écosystème: la formation, d'abord, qui doit permettre de contribuer à pallier la pénurie de talents dans cette filière d'avenir. La donnée, ensuite, dont l'exploitation doit nous permettre d'inventer la cybersécurité de demain. La co-construction, enfin, dont l'efficacité a déjà fait ses preuves et qui doit devenir la norme. Des orientations préfigurant la séquence stratégique qui s'ouvrirait ensuite en interne (voir p. 16).

Les vrais visages de l'ANSSI

Si son évolution est nécessaire, il n'est pas question pour l'ANSSI de renoncer à son essence : celle d'une agence technique et opérationnelle, profondément ancrée dans les enjeux régaliens de la sécurité et de la défense de la nation. Issue de la riche his-

« À l'ANSSI, les jeunes (et les moins jeunes !) qui nous rejoignent ont l'opportunité de progresser, de monter en compétence et de travailler sur une variété de missions. »

JULIE LEDOUX
Cheffe de la division Ressources humaines

toire cryptographique française, elle s'illustre depuis toujours par ses compétences mises au service de la protection du secret. Ces fondements contribuent à la rendre fière.

Dans les murs, cet ADN est associé à une certaine culture du dialogue, du débat (voire parfois du « troll ») et à une ambiance qui repose souvent sur le partage de passions communes. L'agence, c'est le traitement sérieux de sujets sensibles dans une ambiance conviviale. C'est aussi une grande diversité de profils qui s'accordent autour d'un même objectif. Son identité historique et tous les à-côtés qui la rendent vivante constituent en quelque sorte « l'âme de l'ANSSI », qui n'a pas besoin d'être décryptée pour être évocatrice.

Pour attirer, l'agence a des atouts. Elle permet à ses nouvelles recrues de progresser considérablement, en bénéficiant des compétences de leurs collègues, en accédant à des formations et en travaillant sur des missions variées et surtout, uniques. L'ambition affirmée pour 2020 : adapter les processus d'intégration à chaque profil rejoignant l'agence, améliorer la gestion des carrières, soutenir le développement des potentiels et accompagner de mieux en mieux les agents, de leur candidature jusqu'à leur départ de l'ANSSI.

Un des premiers facteurs de motivation à rejoindre l'agence réside dans la finalité de son action. Pour Julie Ledoux, cheffe

de la division Ressources humaines, « *en rejoignant l'ANSSI, on vient mettre ses compétences au service de l'intérêt général, au service d'une mission qui a du sens* ». Pour l'anecdote, l'accueil d'Ortie, future chienne guide en apprentissage auprès d'un agent en 2019, a fait le bonheur des locataires de la tour Mercure. Aussi l'« âme de l'agence » se trouve-t-elle avant tout dans son humanité.

Une agence qui continue d'évoluer

Depuis ses débuts, l'agence est en changement permanent, s'appuyant sur la dernière évolution pour concevoir la suivante. En interne, il s'agit alors de les accompagner et de veiller à préserver une certaine proximité entre chaque échelon à mesure que l'agence grandit. Sachant qu'elle conserve, au plus haut niveau et dans toutes les sous-directions, la volonté d'être une agence responsable et de faire reposer son action sur ses valeurs centrales : compétence, ouverture, agilité.

Il y a dix ans, l'agence comptait à peine une centaine de personnes. Au 31 décembre 2019, elle rassemblait 610 agents. Une croissance qui témoigne de l'intérêt réel des autorités pour la sécurité informatique des instances étatiques et critiques. « *Des moyens qui nous obligent* », répète Guillaume Poupard, pour qui il ne s'agit pas de continuer à croître de façon homothétique, mais bien de « *faire évoluer notre action, pour que la courbe rapportant notre efficacité à nos moyens soit exponentielle* ».

Intégrant ses nouvelles ressources et s'adaptant à son environnement, l'agence a poursuivi en 2019 sa restructuration. Au sein de la sous-direction Opérations (SDO), deux nouvelles entités ont vu le jour pour assurer la mise en oeuvre de dispositifs de détection système et une meilleure prise en compte des menaces de masse (voir pp. 32-37). Poursuivant sa croissance, la sous-direction a « passé la barre » des 200 agents. Un nombre symbolique, vingt ans après la création de son ancêtre, le CERTA*, qui ne rassemblait pas plus d'une quinzaine de personnes.

« En 2020, l'ANSSI lancera une démarche pour amplifier cette dynamique d'innovation dans un esprit d'ouverture et de co-construction. »

JEAN-BAPTISTE DEMAISON
Conseiller innovation auprès du sous-directeur Stratégie

Les autres sous-directions ont également profité de l'année pour poursuivre leur développement, dans la lignée de la nouvelle organisation annoncée fin 2018. La sous-direction Stratégie (SDS) a vu la création d'une cellule de planification stratégique (CPS), dédiée à l'appui au fonctionnement de groupes de travail stratégiques et à l'accompagnement d'entités internes dans leur développement. « *Les porteurs d'activité disposent toujours d'une très bonne vision de leurs enjeux. Ce que nous leur apportons, ce sont des outils et un regard extérieur pour les aider à tirer des orientations structurantes* » résume le chef de cellule Yann Salamon.

La sous-direction Administration (SDA), quant à elle, renforce son activité, à commencer par la fonction RH. Selon les mots de son sous-directeur Michel Babeau, « *SDA se reconstruit pour tendre vers une mission d'accompagnement de la transformation de l'agence.* »

Du côté de la sous-direction Numérique (SDN), des travaux ont été engagés pour la rapprocher du Centre de transmission

* Ancienne appellation du centre gouvernemental français de réponse à incident, ensuite rebaptisé CERT-FR.

gouvernemental (CTG). Le 1er juillet 2020, les deux équipes seront mutualisées au sein d'un opérateur unique, l'OSIIC – Opérateur des systèmes d'information interministériels classifiés – rattaché à la Secrétaire générale de la défense et de la sécurité nationale (SGDSN), avec l'objectif de mieux répondre au besoin croissant de moyens de communication sécurisés. Au sein de la sous-direction Expertise (SDE), enfin, si la structure est restée identique, le développement de collaborations renforcées – avec le nouveau Conseil scientifique, avec l'Institut national de recherche en sciences et technologies du numérique (Inria) – contribue à renouveler les méthodes et les approches (voir pp. 38-47).

Innover collectivement

Au fil des années, l'ANSSI a construit en interne de nombreux comités, croisant les expertises pour garantir la cohérence et la précision de la parole de l'agence. Mais il apparaît aujourd'hui nécessaire d'ajuster l'approche. Quitte à se « mettre en danger », l'agence constate l'intérêt du droit à l'expérimentation, et la nécessité d'ouvrir plus en amont les débats hors les murs. Y compris d'un point de vue purement technique, les spécialistes relèvent qu'il n'existe pas toujours une seule et unique bonne réponse. Aujourd'hui, l'agence n'exclut plus de publier des réflexions et projets en cours de développement.

Décloisonner le débat commence par permettre la transversalité en interne. En 2019, l'ANSSI a pris le parti de donner la parole

aux agents dans le cadre de la démarche d'innovation collaborative ANSSI10+. Une séquence dont les conclusions ont permis l'élaboration du *Manifeste*, récit stratégique de l'agence publié en janvier 2020 (voir p. 16).

Pendant trois mois, l'agence dans toute sa diversité s'est donc réunie à l'occasion d'ateliers d'innovation collaborative, où l'on a cherché à tirer les bonnes ficelles pour faire émerger les bonnes idées. Une première à l'ANSSI, qui illustre une aspiration à trouver de nouvelles méthodes de travail plus à même de créer des synergies.

La séquence a permis de confirmer des orientations déjà latentes, comme celles annoncées le 4 juin 2019, mais aussi de faire émerger d'autres pistes. Ainsi, pendant les ateliers, la question de la collecte, du stockage et du traitement des données techniques a été approfondie et est apparue comme une condition fondamentale de l'efficacité opérationnelle de la communauté cyber (voir pp. 24-31).

« La sécurité est une condition fondamentale à la réalisation des promesses sociales, économiques, citoyennes et démocratiques du numérique. »

MANIFESTE DE L'ANSSI

Autre type de besoin exprimé par les agents : celui de conserver, dans une agence qui grandit, la proximité d'une structure à taille humaine. Et, dans une administration souvent tournée vers l'opérationnel, la nécessité de sanctuariser le temps de la réflexion et de la connaissance a été relevée.

La cybersécurité par de nouveaux prismes

La mise en perspective des actions de l'agence nécessite parfois de faire un pas de côté pour s'ouvrir à des regards inhabituels. L'atelier sur les imaginaires liés à la sécurité, ouvert à l'extérieur, en a été la parfaite démonstration : c'était l'occasion, de façon inédite, de mettre le sujet de la cybersécurité en perspective avec d'autres grandes préoccupations, en particulier les enjeux environnementaux.

L'utilité sociétale des innovations technologiques a également été soulevée,


CLAUDIE HAIGNERÉ ET HUGO HORIOT

Membres du groupe « Talents » de l'Agora 41

« Changer nos regards sur la cybersécurité, inclure davantage ! »

Claudie Haigneré
Conseillère auprès du directeur général de l'Agence spatiale européenne

La cybersécurité est généralement associée à la catastrophe. Et pour cause ! Quand on en parle, c'est souvent en des termes angoissants, parce qu'il est déjà trop tard. Mais l'adhésion ne se construit pas sur la peur. Pour attirer, nous devons construire de nouveaux imaginaires.
Au sein du groupe « Talents », nous croyons que pour préparer l'avenir de la sécurité numérique (et donc notre avenir tout court), il faut d'abord donner envie aux jeunes. Avec son aspiration à la liberté, à la justice et à la protection de l'environnement, la jeunesse est déjà actrice d'un monde plus souhaitable. Notre responsabilité est de faire en sorte que la sécurité numérique devienne un autre de ces grands enjeux mobilisateurs.
L'inclusion des femmes dans ce domaine doit être un sujet à part entière. Car nous ne pouvons nous contenter d'une matière numérique qui serait écrite sans les femmes et la diversité de leurs points de vue.
Apprenons à parler à toutes celles et ceux qui ne vont pas spontanément vers la cybersécurité, par crainte ou par incompréhension des enjeux ! Et faisons-en, enfin, un grand sujet de réflexion et d'action, individuelle et collective. ●

Hugo Horiot
Comédien, réalisateur, écrivain

Pour technique qu'elle puisse paraître, la cybersécurité est avant tout affaire d'hommes et de femmes. Et les enjeux sont tels qu'il est vital d'investir toutes les options pour gagner en efficacité.
Du point de vue des ressources humaines, la prise en compte de la diversité sous toutes ses formes est une clé essentielle de succès. La preuve n'est plus à faire : les équipes diversifiées – par exemple en termes d'âge, de sexe ou d'origine – sont les plus créatives et productives.
Pensons également à la diversité cognitive ! De nombreuses organisations s'intéressent déjà aux profils « atypiques » et les appréhendent comme un véritable atout. Avec un style de traitement de l'information qui leur est propre, certains profils du spectre de l'autisme, par exemple, peuvent apporter une perspective unique et précieuse aux organisations. Malheureusement, de l'école à l'emploi, les écosystèmes et les processus de sélection ont tendance à échouer à détecter les divers potentiels et talents au sein des minorités cognitives en les marginalisant.
En développant un récit et une culture « cyber », en améliorant nos façons d'inclure, nous pouvons permettre à des potentiels inattendus de s'épanouir au sein de nos organisations… dans l'intérêt de tous ! ●

alors que le choix de la déconnexion a souvent été au cœur des scénarios prospectifs élaborés collectivement. La question, presque philosophique, de la finalité des outils numériques dépasse le périmètre de l'ANSSI. Mais elle n'est pas étrangère à la notion de confiance numérique, plus que jamais au cœur de la vision de l'agence.

La volonté affirmée d'anticiper les révolutions d'usage requiert aussi une ouverture affirmée à l'écosystème et, plus largement, à la société. Comme l'ambition de devenir une agence qui soit, plus qu'elle ne l'est aujourd'hui, « orientée bénéficiaires », exigeante mais tenant compte des réalités de ses partenaires.

Cette ouverture aux questions sociétales n'est pas si nouvelle. Elle se fait dans le prolongement d'une démarche existante : l'Agora 41. Ce groupe rassemble 41 personnalités issues de tous les domaines – sauf de la « cyber » – et offre un regard extérieur, souvent inspiré des sciences humaines et sociales. La question de l'attractivité de cette filière pour les femmes, où elles ne sont que trop peu nombreuses, fait, par exemple, partie des sujets soulevés par cette instance satellite de l'ANSSI (voir témoignage p. 15).

Un nouveau récit stratégique

Le 21 janvier 2020, lors de ses vœux, le directeur général a présenté le *Manifeste* de l'ANSSI : une vision stratégique nourrie de ces quelques mois de réflexion, mais reposant sur un socle préexistant la création de l'ANSSI. Ainsi, le modèle français de cyberdéfense distinguant les missions offensives (« l'équipe rouge ») et les missions défensives (« l'équipe bleue ») est un héritage précieux. Ce modèle « *visionnaire* » – selon les mots de Guillaume Poupard – démontre encore qu'il est à l'origine de la confiance accordée à l'agence.

Le positionnement interministériel de l'ANSSI, placée auprès du SGDSN, est aussi ce qui a permis la mise en œuvre de législations ambitieuses. Et si l'ANSSI est écoutée en France, sa voix porte également au-delà des frontières. Sa crédibilité acquise en une décennie lui permet de faire autorité en France et de porter une voix singulière au sein de l'Union européenne.

Dans un contexte numérique extrêmement mouvant, l'agence souhaite désormais se saisir davantage de certaines ruptures profondes, au-delà des bulles médiatiques et des tendances éphémères. Par ailleurs, certains phénomènes observés – prolifération des menaces de masse, amplification des attaques par rebond – obligent, pour assurer la sécurité nationale, à élargir le champ d'action pour aller au-delà des structures les plus critiques.

Pour saisir les opportunités et maîtriser les risques inhérents à ces transformations, l'ANSSI affirme aujourd'hui sa vocation à s'ouvrir davantage à la communauté SSI et au-delà. L'idée qui sous-tend l'ensemble : il devient essentiel pour l'agence, qui ne peut protéger l'ensemble des acteurs de la nation, de faire évoluer son action pour contribuer à la structuration d'un écosystème toujours plus performant. Dans un contexte où de grands acteurs, étatiques ou non, adoptent des stratégies souvent agressives, la filière française et européenne de la sécurité est appelée à faire front, à se structurer et à

610
agents au
31 décembre 2019

118
nouvelles recrues
en 2019

26 %
de moins de 30 ans

coopérer davantage pour gagner en efficacité (voir pp. 18-23).

La nécessité d'irriguer les métiers du numérique ressort aussi comme un enjeu central. Alors que les questions de sécurité sont encore trop souvent prises en compte en aval de la conception, il s'agit, plus que jamais, de promouvoir la « *security by design* » et de conscientiser le monde du numérique… et la société dans son ensemble.

Enfin, si l'agence doit partager ses ressources et son expertise, elle doit également s'enrichir du savoir-faire et des connaissances de ses partenaires. La co-construction, en interne comme en externe, devient alors pour l'agence un maître mot.

Concrétiser l'intention

Pour concrétiser ces orientations, de grands chantiers sont déjà lancés pour les années à venir. Avec l'ambition de se rapprocher des acteurs régaliens de la cyberdéfense – en particulier le Commandement de la cyberdéfense (COMCYBER) et la direction générale de l'armement (DGA) du ministère des Armées – l'ouverture prochaine d'un nouveau site de l'agence à Rennes fait partie des grandes annonces de l'année. L'objectif : y accueillir jusqu'à 200 agents à horizon 2025. En 2020, il s'agira alors d'identifier, en interne, les missions qui pourraient y être localisées afin de construire un projet ambitieux et cohérent pour la cyberdéfense française.

Dernier grand projet et non des moindres : la création du Campus Cyber, une mission confiée par le Premier ministre à Michel Van Den Berghe (voir témoignage ci-contre). Mise en application de la volonté de développer des collaborations au sein de la filière, le Campus prévoit de colocaliser services de l'État, industriels de la cybersécurité et du numérique, laboratoires de recherche, PME, start-up, acteurs de la formation et utilisateurs. Ce « totem » porté par le monde industriel sera ainsi conçu pour stimuler les synergies avec notamment des plateaux projets, un auditorium et un centre de séminaires.

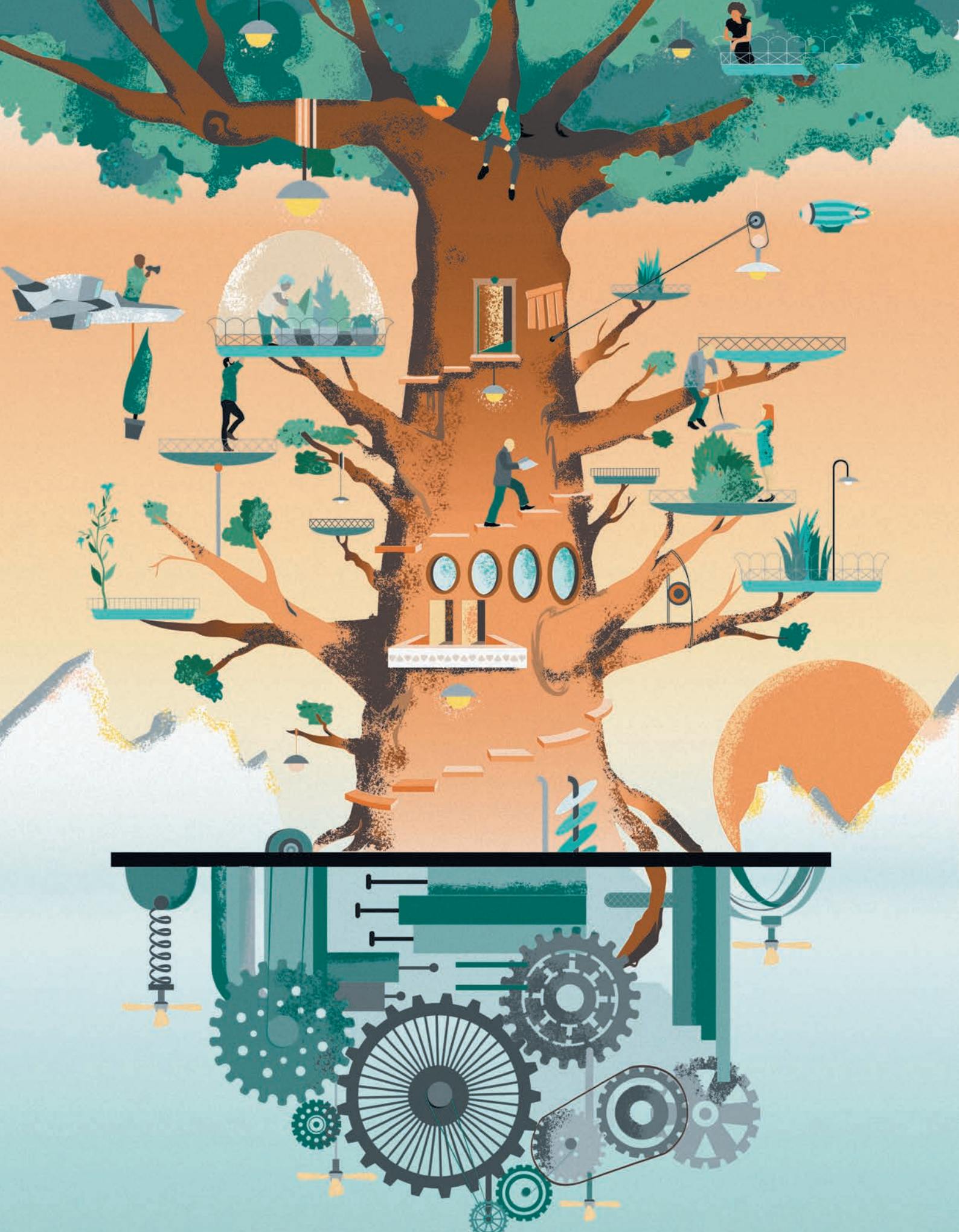
Soutenant pleinement la démarche et amenée à s'y inscrire dès l'ouverture du Campus en 2021, l'ANSSI pourra y transmettre son expertise, développer la connaissance de ses bénéficiaires et se positionner comme une entité fédératrice autour de projets d'intérêt commun. ●

MICHEL VAN DEN BERGHE

Directeur général d'Orange Cyberdéfense, responsable de la mission Campus Cyber

« Pour un centre de gravité de la cybersécurité en France et en Europe. »

Dans un environnement numérique mouvant et parfois hostile, les acteurs de la cybersécurité doivent sans cesse se réinventer. Je suis aujourd'hui convaincu que la clé de notre efficacité se trouve dans la mise en commun des ressources et des expertises – techniques, scientifiques ou sectorielles. Le projet de Campus Cyber constitue d'abord une réponse concrète aux menaces auxquelles nous faisons face, collectivement. C'est un pari : celui du rapprochement des acteurs – start-up, industriels, laboratoires, services de l'État… – qui n'ont certes pas l'habitude de travailler ensemble, mais qui ont énormément à s'apporter ! Le constat est partagé par tous : la création de synergies est désormais une condition indispensable à notre efficacité opérationnelle. Et puis, il y a pour le secteur un enjeu d'image. Ce projet collectif sera un véritable atout pour la visibilité et l'attractivité de notre filière, en particulier face à la pénurie de talents. Et si nous parvenons à accueillir en ce lieu des offres de formation, nous pourrons également rapprocher les jeunes spécialistes de leurs futurs employeurs.
J'émets un point de vigilance : l'objectif n'est pas de faire du Campus une galerie de sponsors ! Il nous faut un campus opérationnel, où les équipes travaillent autour de projets communs. Un véritable lieu de rencontre, qui génère de la vocation. L'ANSSI, avec son expertise, pourra être fédératrice autour de projets d'intérêt général. Pour elle, c'est aussi une occasion de se rapprocher des réalités des acteurs privés pour fluidifier l'émergence de solutions adaptées, au niveau élevé de sécurité. Au-delà de la France, ce grand projet est avant tout un enjeu de souveraineté européenne. Mais le Campus sera aussi ouvert aux acteurs internationaux. Il s'agit bel et bien de bâtir un véritable lieu totem de la cybersécurité, ouvert sur l'Europe et sur le monde. ●



Écosystème : une mobilisation à la hauteur des enjeux

Faire autorité, c'est aussi faire confiance et favoriser le développement d'une dynamique collective capable de s'exercer sur plusieurs terrains, en France comme à l'international. Aussi, et chaque fois que cela est possible, l'ANSSI s'emploie à permettre le développement de nouvelles synergies avec ses partenaires de tous horizons pour interpeller des publics qui lui sont moins familiers et hisser la cybersécurité au rang de priorité stratégique.

En France comme en Europe, dans le public comme dans le privé, auprès des plus petites structures comme des plus grandes... Il importe à chaque échelon de relever le défi de la cybersécurité. En sa qualité d'autorité nationale, l'ANSSI intervient tour à tour et jamais seule comme animatrice, facilitatrice ou promotrice d'une vision française pour voir s'élever partout et au juste niveau la prise en compte du risque numérique.

Une mécanique collective

Le modèle français de cybersécurité se caractérise par une distinction claire entre missions offensives et défensives et s'épanouit grâce à la capacité de tout un écosystème à s'organiser pour élever le niveau global de cybersécurité. Tandis que l'ANSSI exerce une mission renforcée auprès de l'État et des opérateurs d'importance vitale (OIV) et de services essentiels (OSE), un vaste réseau de prestataires complète cet accompagnement en proposant leurs services de détection, d'audit ou encore de réponse à incidents. Parmi eux, certains sont détenteurs d'un visa de sécurité délivré par l'agencew. À terme, le visa valorisera une nouvelle catégorie de services en s'adressant aux prestataires d'administration et de maintenance sécurisées (PAMS) des systèmes d'information. En 2019, le référentiel d'exigences applicables aux PAMS a fait l'objet d'un appel à commentaires public en vue d'être testé en conditions réelles auprès de prestataires volontaires.

Lorsque survient un événement de sécurité, sa nature, sa criticité ou encore le statut de la victime déterminent le niveau d'intervention de chaque acteur. Récemment, l'ANSSI a par exemple observé les conséquences d'une attaque par rançongiciel (voir pp. 32-37) sur des secteurs aussi variés que la santé, les médias ou l'industrie agroalimentaire, pour n'en citer que quelques-uns. Pareilles circonstances sont souvent l'occasion pour l'agence de développer sa connaissance de l'état de la menace en bénéficiant du retour d'expérience des entités victimes et des experts mobilisés pour résoudre l'incident.

« Il s'agit de faire évoluer notre approche, notre action comme nos modes d'intervention pour davantage tirer parti de cet écosystème en construction et grandir collectivement. »

MANIFESTE DE L'ANSSI

VISAS DE SÉCURITÉ

198
Visas délivrés dont :

95
certifications

103
qualifications

L'entrée en vigueur le 1er janvier 2019 de la loi de programmation militaire 2019-2025 marque quant à elle l'ajout d'un nouveau rouage à cette mécanique. Le second volet de l'article 34 de la loi autorise l'ANSSI, lorsqu'elle a connaissance d'une menace grave et imminente sur les systèmes d'une autorité publique, d'un OIV ou d'un OSE, à déployer un dispositif de détection sur le serveur d'un hébergeur ou l'équipement d'un opérateur de communications électroniques sur une durée et un périmètre limités. Cette nouvelle mission s'effectue sous le contrôle de l'Autorité de régulation des communications électroniques et des postes (ARCEP).

En anticipation des grands rendez-vous aussi, la réponse collective s'organise. Compétitions sportives, échéances électorales, sommets internationaux… Ces événements à forts enjeux auxquels participe la France sont exposés à toutes sortes de risques, y compris numériques. En 2019, les élections européennes et la tenue du G7 à Biarritz ont ainsi fait l'objet d'un accompagnement spécifique de la part de l'agence en coopération avec les services de l'État. Dans le cadre du G7, l'agence tout entière s'est mobilisée pour accompagner au mieux la Présidence de la République dans la prise en compte au juste niveau des mesures de cybersécurité relatives au sommet : conception, exploitation et supervision de sécurité du système d'information de l'événement ; limitation au strict nécessaire des services en ligne ;

« La conscience et la maîtrise du risque numérique deviennent des fondamentaux pour assurer, demain, la résilience et l'immunité collectives des organisations. »

YANN TONNELIER
Chef adjoint du bureau Management des risques cyber

information et sensibilisation des participants ; organisation et préparation de la gestion de crise ; etc.

Management du risque numérique : là où tout commence ?

Marteler que « *la cybersécurité est l'affaire de tous* » ne suffit pas, encore faut-il la rapprocher des préoccupations et responsabilités de chaque acteur. En matière de sécurité numérique, la méthode d'analyse de risque EBIOS *Risk Manager* ouvre la voie en offrant aux acteurs opérationnels et aux dirigeants une compréhension et une responsabilité partagées des risques numériques (voir Rapport d'activité 2018). La méthode constitue ainsi le pilier de la doctrine de management du risque numérique de l'ANSSI. De plus en plus, les principes de la méthode – du socle de sécurité au traitement du risque en passant par son appréciation – innervent ainsi les pratiques des acteurs de la sécurité numérique et de la gestion du risque.

Toutefois, EBIOS *Risk Manager* constitue le moteur d'une mécanique plus complexe qui doit impliquer chaque acteur, à commencer par les dirigeantes et dirigeants de structures publiques ou privées. L'établissement de ce besoin part d'un constat assez simple : demain, l'organisation responsable et génératrice de confiance sera celle qui s'attache à maîtriser le risque numérique pour elle-même et pour son écosystème. Cela suppose pour les directions de comprendre ce

« Nous devons encore plus être une “administration orientée bénéficiaires” pour toujours mieux comprendre les besoins, les attentes, mais également les contraintes des bénéficiaires de notre action. »

MANIFESTE DE L'ANSSI

risque pour ensuite soutenir les mesures nécessaires voire, dès lors qu'un certain niveau de maturité est atteint, faire connaître et valoriser cet investissement. Partenaires de longue date, l'ANSSI et l'Association pour le management du risque et des assurances de l'entreprise (AMRAE) ont donc décidé de mettre en commun leurs compétences pour proposer une démarche capable d'accompagner les dirigeantes et dirigeants dans l'établissement ou la consolidation d'une politique de gestion du risque numérique. Décrite dans le guide *Maîtrise du risque numérique – L'atout confiance*, la démarche issue de cette collaboration a été pour la première fois présentée en novembre 2019 lors du Forum européen FERMA qui réunit chaque année associations européennes de management du risque et professionnels de l'assurance. Un lancement européen qui n'a rien d'un hasard puisque la France fait régulièrement valoir dans les enceintes européennes la maturité de son approche sur ces enjeux devenus indissociables.

L'Europe d'abord

Dans un nombre croissant de domaines, l'Europe constitue l'échelon naturel et souhaitable pour promouvoir une vision souveraine de la cybersécurité et exprimer ses valeurs sur la scène internationale. En plaidant pour une approche ambitieuse de la cybersécurité tournée vers l'économie et la société, l'ANSSI participe à modeler les législations européennes et à développer les enceintes d'échange en la matière.

En 2017, la Commission européenne adoptait une recommandation dénommée *Blueprint* dont l'objectif est d'inviter les États membres et les institutions européennes à organiser la coopération et l'échange en matière de gestion de crise cyber aux niveaux politique, opérationnel et technique. Premier-né de ces organes d'échange, l'exercice Blue OLEx s'est tenu à Paris les 2 et 3 juillet 2019 à la suite d'une initiative conjointe et inédite de la France et de l'Espagne. Au cours de ces deux journées, les responsables d'autorités nationales de cybersécurité de l'Union européenne, la Commission européenne et l'ENISA, l'Agence européenne pour la cybersécurité, se sont livrés à un exercice sur table visant à adresser le niveau opérationnel de la gestion de crise cyber. En résulte l'établissement de nouveaux principes et procédures de coopération visant à mieux organiser la gestion collective des crises d'origine cyber impactant les pays européens. Pour preuve, la mobilisation observée pendant et à l'issue de l'exercice conduit désormais les acteurs de ce réseau à penser les modalités de pérennisation de ce dialogue entre autorités et à optimiser les flux d'échange à chaque niveau de la gestion de crise. La seconde édition de Blue OLEx est programmée aux Pays-Bas en 2020 (voir témoignage ci-contre). D'un point de vue plus technique cette fois, l'exercice CyberSOPex2019 (SOP pour *Standard Operative Procedures*) organisé par l'ENISA a une nouvelle fois démontré la qualité de la coopération inter-CERTs à l'échelle européenne en la mettant à l'épreuve face à des scénarios d'attaque de masse.

Parmi les sujets ayant animé les concertations européennes, impossible de faire l'impasse sur l'émergence de la 5G en Europe. En plus d'accélérer de manière considérable le débit des communications sans-fil, cette

Forum FERMA 2019 à Berlin : Brigitte Bouquot, présidente de l'AMRAE, et l'ANSSI présentent une vision partagée du management du risque numérique.

« Nous devons renforcer notre engagement européen pour accélérer la construction d'une Europe de la cybersécurité, en complémentarité avec l'échelon national. »

MANIFESTE DE L'ANSSI

technologie de rupture intègre de nouveaux usages inédits qui, à terme, pourraient avoir des conséquences significatives dans des secteurs d'activité aussi critiques que la santé, l'énergie ou encore les transports. Si la sécurité des réseaux 5G renvoie inévitablement vers des problématiques de sécurité nationale, elle n'en demeure pas moins un enjeu de souveraineté européenne fondé sur le partage d'une vision et de valeurs communes. Cette posture a présidé à la conduite de discussions entre les États membres, la Commission européenne et l'ENISA. La « boîte à outils 5G » qui en résulte (*5G Toolbox*) rassemble un arsenal de mesures stratégiques et techniques partagées, ainsi qu'un plan d'action permettant à chaque État membre d'établir un plan de maîtrise des risques associés à cette technologie.

Preuve de la transversalité de l'approche française et de ses valeurs à chaque échelon – national, européen et international – la France n'a de cesse de rappeler sa vision du cyberespace et des forces en présence. Dans la lignée de l'Appel de Paris pour la confiance et la sécurité du cyberespace lancé en 2018 par le président de la République, l'Organisation de coopération et de développement économiques (OCDE) a organisé en novembre 2019 un forum sur ces mêmes enjeux. À cette occasion, Guillaume Poupard et Henri Verdier, ambassadeur pour le numérique, ont tenu à rappeler leur attachement à ne pas voir se développer un « Far West numérique ». ●

PATRICIA ZORKO

Coordinatrice nationale adjointe pour la sécurité et la lutte contre le terrorisme, Pays-Bas

« L'UE a un rôle essentiel à jouer dans la transformation numérique de nos économies et sociétés et de ses enjeux. »

Le modèle de cybersécurité néerlandais repose sur un réseau décentralisé et des partenariats public-privé. Les secteurs, conscients de leurs besoins et spécificités propres, s'organisent eux-mêmes en communautés de confiance et sont nombreux à disposer de leurs propres CERTs informés par le NCSC-NL.
Aux Pays-Bas, nous souhaitons faire de la cybersécurité un enjeu à part entière du quotidien des organisations publiques ou privées. Cela nécessite une forte coordination nationale pour que chacune prenne ses responsabilités dans l'intérêt commun.
Ces dernières années, l'Europe a accompli d'importants progrès en la matière sous l'impulsion de textes tels que la directive européenne *Network and Information Security* (NIS), le *Cybersecurity Act* ou la recommandation *Blueprint.* Tout cela exige du *leadership*, de la coordination et une capacité à traduire des actes juridiques en actions tangibles. Nous étions ravis que la France organise l'exercice Blue OLEx en 2019, mette à l'épreuve notre préparation commune et nous réunisse à un niveau stratégique. Je dis toujours : faites-vous des amis avant d'en avoir besoin ! Nous sommes très heureux de pouvoir perpétuer cette tradition établie par nos amis français en organisant la prochaine édition de cet exercice.
L'UE a un rôle essentiel à jouer dans la transformation numérique de nos économies et sociétés et de ses enjeux. Le cyberespace est dépourvu de frontières, les États membres ne peuvent donc pas se contenter d'affronter ces enjeux seuls. Ensemble, nous devons permettre aux citoyens européens de tirer parti de ces technologies tout en assurant la protection de nos réseaux et droits fondamentaux. Notre effort commun sur la *Toolbox* 5G est le parfait exemple d'une coopération réussie à l'échelle européenne et j'espère que d'autres projets suivront cette même voie. ●

La connaissance : objet de cycles et de métamorphoses

C'est en train de devenir une philosophie pour l'ANSSI : partager ses connaissances chaque fois que cela est possible. Étonnant pour une agence dont l'activité s'est construite sur la culture du secret, serions-nous tentés de penser... Et pourtant ! L'expertise acquise au fil des ans, les données techniques et opérationnelles, ou encore les travaux de R&D sont autant de connaissances et savoir-faire qui s'enrichissent et se transforment au contact d'autres acteurs. Plus que jamais, l'ANSSI souhaite embrasser ce modèle pour, collectivement, stimuler l'innovation, renforcer la cybersécurité d'aujourd'hui et inventer celle de demain.

Mettre en commun ce qui peut l'être va de pair avec la responsabilité qui incombe à l'ANSSI. « *La cybersécurité est l'affaire de tous !* » se plaît à rappeler Guillaume Poupard. Loin d'être désuète, la formule prend, de plus en plus, des formes très concrètes. Si l'agence a toujours eu à cœur de tenter de partager ses connaissances et ses outils (doctrine technique, connaissance de la menace, moyens de communication sécurisés…), les ressources produites ont longtemps ciblé presque exclusivement ceux qui avaient déjà atteint un haut niveau de maturité. C'est toujours en partie vrai, mais l'ANSSI ouvre désormais un nombre croissant de données et de projets pour voir la communauté s'en emparer, les faire fructifier et ainsi contribuer à élever le niveau global de cybersécurité.

De quelles données parle-t-on ?

Le 4 juin 2019, lors du Cyber Festival célébrant les dix années d'existence de l'ANSSI, Guillaume Poupard plaidait pour « *l'ouverture, le partage et la mutualisation responsables de certaines données techniques* », jusqu'à en faire une priorité stratégique pour l'agence. « Tada ! La magie de la donnée », c'est d'ailleurs le nom donné à l'un des ateliers organisés dans le cadre de la démarche ANSSI10+. Bien que le mot soit aujourd'hui dans toutes les bouches, l'agence a souhaité réfléchir à ce que la donnée de cybersécurité signifie pour elle et son écosystème.

Les données de cybersécurité détenues par l'ANSSI sont principalement issues d'activités telles que la réponse à incidents, la détection* ou encore l'assistance technique. Une fois analysée, cette matière brute vient enrichir les connaissances de l'agence et irriguer ses travaux. L'objectif ? Demeurer à l'état de l'art pour toujours mieux comprendre, anticiper et prévenir la menace. S'il n'est évidemment ni possible ni souhaitable de toutes les partager, il n'est plus à prouver que, dans de nombreux cas, la mise en commun de données brutes, de connaissances ou d'outils participe au renforcement de la confiance et de la sécurité collectives.

57
formations SecNum*edu* labellisées
et
16 000
attestations SecNum*académie* délivrées au 31 décembre 2019

Près de
80
guides techniques et recueils de bonnes pratiques disponibles
et
6
rapports publiés sur les menaces et incidents au 31 décembre 2019

« Les évolutions législatives de ces dernières années confient à l'ANSSI un accès à des volumes croissants de données techniques de cybersécurité, d'une valeur exceptionnelle. »

MANIFESTE DE L'ANSSI

La transmission, un facteur clé de succès

En France, le développement de la sécurité numérique est freiné par le manque de personnes formées à ces métiers. Il s'agit pourtant d'une filière d'avenir pour quantité de profils, principalement techniques, mais pas seulement. Le Centre de formation à la sécurité des systèmes d'information (CFSSI) de l'ANSSI agit donc en faveur de cet essor en proposant aux agents publics ainsi qu'aux personnels des opérateurs d'importance vitale et de services essentiels (OIV et OSE) un catalogue d'une trentaine de formations. Parallèlement, il participe à la structuration

de l'offre nationale par la labellisation SecNum*edu* de formations spécialisées et le programme SecNum*edu*-FC pour les formations continues. Le MOOC SecNum*académie* continue quant à lui de faire école et a déjà sensibilisé, depuis sa création en 2017, plus de 125 000 personnes aux fondamentaux de la sécurité des systèmes d'information.

Autre fait majeur, la cybersécurité a désormais fait son entrée dans les programmes et manuels scolaires ! Ainsi, les programmes d'histoire-géographie ou encore la nouvelle matière sciences numériques et technologie (SNT) dispensés au lycée font découvrir aux élèves les enjeux et puissances à l'œuvre sur ce territoire nommé cyberespace. Les collégiens sont quant à eux de plus en plus nombreux à se familiariser avec les bonnes pratiques de sécurité numérique ou à découvrir les secrets de fabrication d'un algorithme en cours de mathématiques. Si ces évolutions sont une excellente nouvelle pour la filière, elles nécessitent d'être accompagnées, en particulier auprès du corps enseignant. C'est pourquoi, le 11 juin 2019, des spécialistes de la cybersécurité (ANSSI, cybermalveillance.gouv.fr, etc.) et de l'éducation (enseignants, experts pédagogiques, chercheurs, etc.) se sont donnés rendez-vous au Lab110Bis, le laboratoire d'innovation du ministère de l'Éducation nationale et de la Jeunesse. Au cours d'ateliers et en présence du ministre Jean-Michel Blanquer, les participants ont orienté leurs réflexions sur l'élévation des compétences en cybersécurité chez les plus jeunes et le renforcement de l'attractivité de la filière. En résulte une feuille de route autour de laquelle s'organisent désormais les actions qui, demain, concourront à enrichir l'arsenal pédagogique des enseignants, ressources ludiques et interactives, dispositifs d'évaluation des compétences, rendez-vous thématiques, etc.

Les professionnels de l'éducation et de la cybersécurité, réunis au Lab110Bis, reçoivent la visite de Jean-Michel Blanquer et de Guillaume Poupard.

« Il est primordial de développer une culture de la sécurité numérique à chaque âge à travers les programmes scolaires, le jeu, le développement de ressources pédagogiques… La cybersécurité est un sujet absolument passionnant et concret à aborder sous quantité d'angles. »

NICOLAS ESLOUS
Coordinateur sectoriel pour l'enseignement et la recherche

Le Service national universel (SNU) voulu par le gouvernement s'adresse aux jeunes de 15 à 17 ans. Deux mille jeunes ont expérimenté en juin 2019 la première phase du programme qui comprend un module dit « cyber ». Pour le réaliser, la direction du Service national et de la Jeunesse a fait appel aux compétences du COMCYBER et de l'ANSSI. Le module issu de ces travaux vise à informer les jeunes sur la cybermenace (origines, motivations) et à échanger sur leurs usages. Un rappel des bonnes pratiques de sécurité numérique vient conclure cette intervention qui devrait être expérimentée à plus grande échelle à horizon 2021.

Pour la troisième année consécutive, le *European Cybersecurity Challenge* (ECSC) continue d'attirer un nombre croissant de jeunes entre 14 et 25 ans. Pour les jeunes Français, la sélection nationale pour intégrer l'équipe France est une occasion inédite d'éprouver leurs compétences en relevant les épreuves conçues par l'ANSSI. En se mesurant individuellement ou collectivement à celles-ci, ils font l'expérience à la fois technique et humaine de certaines réalités rencontrées par les experts de la cybersécurité.

De la théorie… à la pratique !

Pour l'ANSSI, les publications ont toujours constitué une excellente manière de restituer et diffuser les connaissances et les savoir-faire. Au rythme d'une dizaine de publications par an, l'agence met ainsi à la disposition de chacun des ressources (guides, MOOC, infographies, etc.) dont les thématiques et les cibles varient en fonction du besoin observé. Pour le qualifier, mobiliser les expertises nécessaires et disposer d'une vue globale sur cette activité, un comité éditorial composé de représentants de chaque sous-direction informe l'interne, assure la revue des projets en cours et en instruit de nouveaux. De plus en plus systématiquement, les publications issues de ce processus font l'objet de consultations avant parution auprès d'un panel représentatif de la cible du document. En 2019, ce fut par exemple le cas du guide de *Bonnes pratiques à l'usage des professionnels en déplacement* publié en partenariat avec le ministère de l'Europe et des Affaires étrangères. Ce dernier a ainsi pu bénéficier des retours de salariés, d'entrepreneurs, de membres d'ONG, d'agents de l'État ou encore d'étudiants pour être au plus près des réalités de chacun.

« Dans un monde où les compétences numériques deviennent des fondamentaux, la cybersécurité doit également être renforcée dans les enseignements scolaires, notamment pour susciter les vocations dès le plus jeune âge. »

MANIFESTE DE L'ANSSI

Les bonnes pratiques de sécurité numérique se retrouvent aussi dans les moyens de communication sécurisés conçus et déployés par la sous-direction Numérique (SDN) et le Centre de transmissions gouvernemental (CTG) qui formeront bientôt le nouvel opérateur OSIIC. Ainsi, en 2019, à un rythme différencié, les solutions ISIS (intranet sécurisé interministériel) et OSIRIS (téléphonie fixe sécurisée de niveau Confidentiel-Défense) ont été déployées en ambassades. Instruites et développées par la SDN, ces solutions sont ensuite configurées conjointement avec le CTG qui intervient sur leur mise en service opérationnelle et leur supervision. Dans ce contexte précis, l'acheminement des équipements par valise diplomatique ainsi

que leur déploiement sur site ont été assurés par le Quai d'Orsay.

En août 2019, lors du G7 qui s'est tenu à Biarritz, les participants ont eu l'occasion d'utiliser un certain nombre de ces outils puisqu'étaient mises à leur disposition des solutions telles qu'ISIS, Horus (visio-conférence) ou encore Tchap, la messagerie instantanée de confiance de l'État développée par la direction interministérielle du numérique (DINUM). Cet évènement a d'ailleurs mobilisé l'ANSSI au-delà de la seule mise à disposition de ces outils. En effet, la sensibilité et l'exposition de l'évènement ont nécessité une préparation et un accompagnement au long cours pour le préserver d'éventuelles menaces d'origine cyber (voir pp. 18-23).

*Open source** et solutions autonomes : le développement… durable ?

En matière de logiciel libre, l'ANSSI compte parmi les plus grands contributeurs de l'État. Si cet engagement n'est pas nouveau, il constitue désormais un principe de développement privilégié pour l'agence. Il existe plusieurs raisons à cela : la réponse à un réel enjeu de sécurité et de souveraineté, la maîtrise de technologies clés, mais aussi

« Il convient d'explorer la possibilité de développer une plateforme hébergée par l'agence, où des services seraient développés par d'autres au profit de nos bénéficiaires, en valorisant les données dont nous disposons. »

MANIFESTE DE L'ANSSI

des possibilités inédites d'évaluation et de diffusion autour de cas d'usage spécifiques. Quand elle ne contribue pas elle-même aux projets entrepris par des tiers, l'ANSSI publie les siens pour que la communauté s'en empare. En la matière, l'année 2019 s'est révélée particulièrement riche avec l'ouverture d'outils couvrant une variété de besoins, de la sécurité des objets connectés à l'analyse de la cybermenace en passant par la réponse à incidents. Les projets qui suivent sont notamment venus rejoindre CLIP OS, le système d'exploitation durci sur Linux que l'agence développe depuis 2006 et dont la version 5 désormais disponible est entièrement conçue sur une base *open source*.

Le projet Wookey a ainsi fait son apparition dans le paysage du libre. Ce disque dur USB chiffrant sécurisé apporte la preuve par l'exemple qu'il est possible, pour un coût raisonnable, de conjuguer expérience utilisateur et sécurité. Ce protocole et l'ensemble des éléments qui le composent peuvent être mis à profit dans le cadre de projets liés aux systèmes embarqués ou aux objets connectés afin de favoriser l'intégration de la sécurité dès la conception.

Pour faire face à de nouvelles formes d'incidents et aux besoins qui en émanent en matière d'investigation et de réponse à incidents, l'agence a conçu en 2011 le logiciel DFIR ORC (pour outil de recherche de compromissions). Intégralement libre depuis 2019, il regroupe un ensemble d'outils qui permettent la recherche, l'extraction et la mise à disposition des données forensiques (analyse post-incident des données du système) en environnement Microsoft Windows. Après huit années d'utilisation pour ses besoins propres, l'agence souhaite ainsi contribuer à la vie de la communauté de la réponse à incident en lui donnant

* Les expressions « *open source* » ou « libre » sont souvent utilisées de manière indifférenciée pour désigner un programme dont le code source est distribué sous une licence permettant son exploitation par des tiers. Néanmoins, il est admis qu'un logiciel dit « *open source* » renvoie davantage à un objectif de développement collaboratif. L'ANSSI met à disposition de la communauté les codes sources de ses projets appartenant à cette catégorie sur GitHub.

la possibilité de favoriser la montée en maturité de la solution et l'apparition de nouvelles fonctionnalités.

Le projet OpenCTI (pour *Open Cyber Threat Intelligence*) a lui aussi beaucoup fait parler de lui ! Solution libre pour traiter et partager la connaissance en matière d'analyse de la cybermenace, OpenCTI est né d'un partenariat entre l'ANSSI et le CERT-EU (voir témoignage ci-contre). Les acteurs de la *threat intelligence* recueillent et développent quantité d'informations stratégiques, opérationnelles et techniques liées aux cybermenaces afin de toujours mieux les anticiper et y répondre. Pour permettre une exploitation efficace de ces connaissances, il s'agissait pour l'agence et le CERT-EU de développer une solution capable de les structurer, les stocker, les organiser, les visualiser et les partager. À terme, l'usage généralisé de la plateforme par les partenaires de l'ANSSI favorisera le développement d'une vision collective de la menace.

De plus en plus et en particulier pour les opérateurs publics réglementés, l'agence souhaite rassembler sous la bannière « Club SSI » un ensemble de prestations visant à renforcer leur sécurité. Le service *Active Directory Security* (ADS) fait partie de celles-ci. L'objectif est d'auditer, à la demande de ces opérateurs et de manière autonome, le niveau de sécurité des annuaires *Active Directory*. Pour la chaîne SSI des acteurs concernés, ADS leur permet de disposer d'une vue globale et synthétique de ce niveau de sécurité. Par extension, le service accompagne le durcissement progressif de l'annuaire par l'application de mesures adéquates, tout en constituant un outil précieux d'aide à la décision pour les dirigeants qui pourront s'appuyer sur l'analyse des résultats fournie. ●

SAÂD KADHI

Chef du CERT-EU

« Changez votre fusil d'épaule, investissez dans l'humain ! »

Ingénieur d'origine marocaine, j'ai toujours baigné dans une culture francophone et c'est en France que j'ai terminé mes études. Mes expériences successives, de Danone à la Banque de France, ont constitué de formidables terrains d'apprentissage et de créativité. C'est là, en créant ou en développant leurs équipes de cyberdéfense, que je me suis résolument engagé dans la transmission et le partage des connaissances. Cette volonté m'a d'ailleurs conduit, avec d'autres, à développer le projet TheHive, qui poursuit le même objectif et connaît désormais un vrai succès. Début 2019, je suis devenu le chef du CERT-EU. Ce n'est pas un « super CERT » de l'Union européenne, mais celui de tous ses organes, agences et institutions comprises. Je cherche à instaurer un véritable cercle vertueux de confiance avec nos pairs et partenaires principaux, car nous sommes plus forts ensemble. Or je constate que certaines barrières psychologiques demeurent dès qu'il s'agit de partager de l'information sur les attaques. J'ai un rêve : celui de voir émerger une sorte de tiers de confiance qui recueillerait ces informations, en vérifierait la qualité, intègrerait certaines limites de diffusion et les fusionnerait avec d'autres données avant de les transmettre. Cela serait un très bon moyen d'accélérer la circulation d'informations de qualité pour contrecarrer les menaces actuelles, telles que les APT, ou futures. Je pense notamment à celles qui pourraient tirer parti de l'IA ou renverser un algorithme pour attaquer ce qu'il est censé défendre. Mais aujourd'hui, j'appelle surtout les entreprises à se réveiller. Soyez critiques et, plutôt que d'investir dans quantité de « solutions » de cybersécurité qui peuvent elles aussi fragiliser vos systèmes d'information, investissez dans l'humain ! ●

La meilleure défense… c'est la défense !

La mission de cyberdéfense de l'agence emporte avec elle un ensemble de représentations particulières : l'ADN régalien, le feu de l'action face à la menace, le sceau du secret. Si bien que dans le souci de préserver les victimes, les éléments publics de réaction aux cyberattaques ne peuvent être que partiels. Sans décrypter dans son entièreté la complexité de la chaîne opérationnelle, il est toutefois nécessaire de donner du sens et d'éclairer cette mission collective sur la base du contexte de la menace… et de considérations humaines.

En quelques années seulement, la transformation numérique a largement redéfini l'organisation de nos sphères personnelles comme professionnelles. De plus en plus, l'interconnexion des systèmes informatiques, l'externalisation et la multiplication des objets connectés – du smartphone à la montre en passant par la télévision – augmentent, de fait, la surface d'attaque… générant inévitablement de nouveaux risques. D'autant que l'enjeu de la sécurisation a tendance à être pris de vitesse par le rythme des innovations technologiques.

Parallèlement, le contexte géopolitique évolue et l'on voit les États intégrer de plus en plus le « cyber » à leur stratégie comme un outil régalien d'influence, de renseignement, voire de domination. Dans son *Manifeste* (voir pp. 8-17), l'ANSSI l'atteste: « *la maîtrise du cyberespace devient l'une des clés de puissance dans le monde à venir* ». Et au-delà des États qui recherchent une forme de supériorité – si ce n'est de suprématie – dans le cyberspace, de grands acteurs privés ne cachent pas non plus leurs ambitions hégémoniques.

Le fonctionnement quotidien de nos organisations et de nos sociétés se trouve, de fait, mis en danger – les pires scénarios d'anticipation allant jusqu'à faire craindre pour la vie de nos concitoyennes et concitoyens. Mais il existe des raisons d'avoir confiance en l'avenir. Car en parallèle, l'écosystème de la cybersécurité poursuit sa montée en puissance, et la société sa prise de conscience.

Une menace évolutive

Pour mieux anticiper et réagir aux attaques, l'ANSSI mène en profondeur et en continu un travail de veille et d'analyse de la menace. Dans une démarche d'ouverture et de partage, des rapports d'analyse sont désormais publiés sur le site du CERT-FR (voir pp. 56-57). Les trois tendances les plus affirmées pour l'année 2019 sont synthétisées ci-après.

« Plus notre société se numérise, plus elle s'expose aux risques inhérents à ces technologies. »

MANIFESTE DE L'ANSSI

RANÇONGICIELS VISANT LES ORGANISATIONS

En 2019, les attaques par rançongiciels ont constitué la menace informatique la plus préoccupante. De plus en plus ciblées vers les entreprises et organisations publiques, elles ont pu être dirigées vers des systèmes d'information critiques. Un constat qui invite l'ANSSI et ses partenaires à reconsidérer les frontières jusqu'alors délimitées entre cybercriminalité et sécurité nationale. Les compromissions par rançongiciel peuvent en effet avoir des conséquences alarmantes, lorsqu'elles touchent par exemple le domaine de la santé ou plusieurs dizaines de victimes simultanément. Mais à ce « jeu », aucun secteur n'est épargné.

Au préjudice de l'attaque s'ajoutent les risques liés à l'exposition médiatique et les possibles pertes économiques en cas d'interruption de l'activité. Mais le paiement de la rançon ne garantit pas le déchiffrement des données, pas plus qu'il ne protège la victime contre une attaque ultérieure. Pire, il renforce le modèle économique des cybercriminels.

ESPIONNAGE

Les opérations d'espionnage se poursuivent avec une tendance à la hausse, la recherche d'informations stratégiques sur les politiques extérieures et de défense demeurant la motivation principale des attaquants. L'accès aux informations industrielles et aux secrets commerciaux des organisations constitue aussi une motivation importante, comme le vol de données personnelles.

En 2019, les tensions géopolitiques ont également suscité des opérations de pré-positionnement de codes malveillants, de reconnaissance des systèmes, voire de sabotage.

ATTAQUES INDIRECTES PAR *SUPPLY CHAIN*

L'année 2019 a confirmé la montée en puissance des attaques indirectes exploitant les relations de confiance entre partenaires. Pour atteindre leur cible finale, des acteurs étatiques comme cybercriminels font désormais souvent le choix d'attaquer l'une de ses parties prenantes (entreprises de services numériques, fournisseurs d'accès Internet, sociétés d'infogérance…).

Cette stratégie constitue pour les attaquants un moyen de contourner les défenses des grandes organisations, réputées plus solides. Elle leur permet également d'obtenir un accès vers d'autres cibles, démultipliant ainsi la portée de leur action.

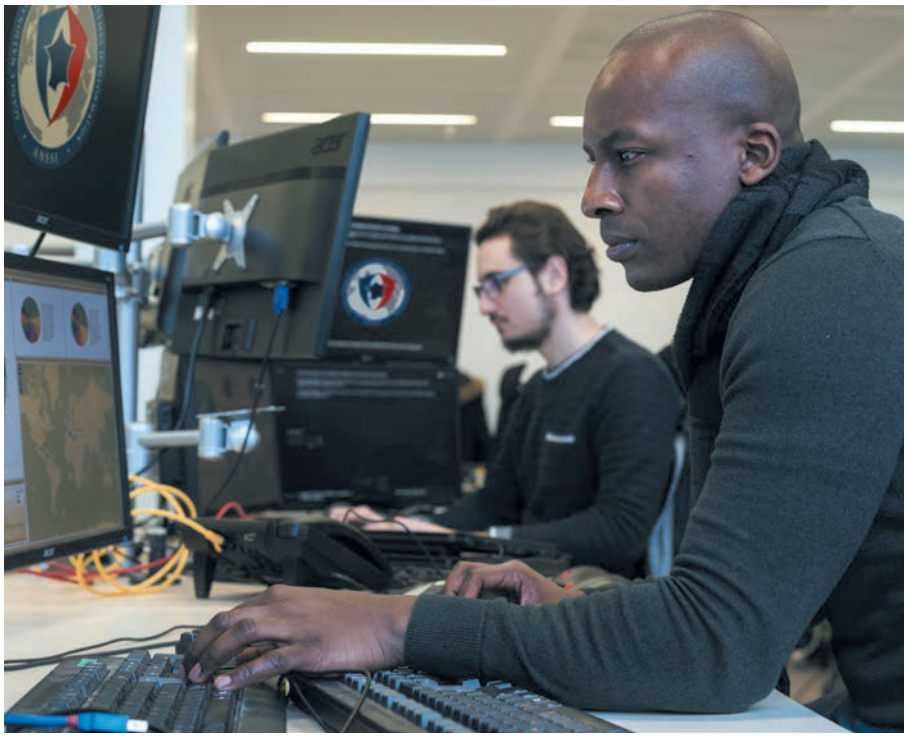
Perfectionner la chaîne opérationnelle

L'ANSSI est aujourd'hui plus efficace et résiliente qu'elle ne l'a jamais été. Cette progression réside pour beaucoup dans ce que Serge Lefranc – le chef de la division Réponse – appelle « *la professionnalisation des métiers de la réponse à incident* ». Par essence, la réponse aux attaques ne se planifie pas. Il s'agit donc, pour l'ANSSI et plus particulièrement pour sa sous-direction Opérations (SDO), de limiter au maximum les zones d'incertitude. Par exemple, en consacrant un effort plus important au suivi de l'activité, à la coopération avec les prestataires ou au partage de données techniques (voir pp. 24-31).

L'organisation de la SDO est comparée, dans ses murs, au mouvement d'un *handspinner*. Alimentées par une mission centrale, trois branches se succèdent et s'interopèrent tout à la fois : la connaissance, la détection et la réponse. Ce sont là les trois piliers de la cyberdéfense – correspondant aux trois divisions de la SDO.

« Du fait de l'amélioration de nos modes d'organisation, un évènement qui aurait nécessité énormément de ressources il y a quelques années est absorbé plus facilement aujourd'hui. »

SERGE LEFRANC
Chef de la division Réponse



La réaction aux cyberattaques mobilise, par ailleurs, de nombreuses expertises au-delà de la SDO. La communication de crise cyber est ainsi l'une des grandes compétences « développées maison », et un service à part entière apporté par l'ANSSI à ses bénéficiaires. En plus de l'expertise technique apportée en cas d'attaque et des impacts d'un tel évènement en termes de perception, l'accompagnement en communication est en effet pleinement intégré au dispositif de traitement des opérations.

D'autres entités pourraient être invoquées à titre d'exemple pour illustrer la transversalité de la réaction aux cyberattaques à l'ANSSI : la division Coordination sectorielle, qui apporte la connaissance des domaines d'activité affectés ; la division Assistance technique, qui accompagne les victimes dans la durée ; la cellule d'anticipation cyber, qui coordonne les opérations au niveau stratégique. Cette action collective se matérialise particulièrement lors de la préparation d'évènements d'ampleur nationale, comme ce fut le cas en 2019 pour la sécurisation des élections européennes ou du sommet du G7 (voir pp. 18-23).

Une réaction organisée

Dans le jargon de l'agence, on distingue différents niveaux d'engagement opérationnel, du moins au plus critique : signalement, incident, incident majeur, jusqu'à l'opération de cyberdéfense. Au sein de la division Réponse de la SDO, le premier maillon de la chaîne opérationnelle assure la veille, réceptionne les signalements et traite les évènements dont les effets sur les systèmes d'information sont considérés comme étant les moins critiques. Quand la gravité de l'évènement de sécurité dépasse un certain seuil, le signalement est acheminé jusqu'aux entités les plus à même de s'en emparer. C'est alors une organisation matricielle, avec des rôles bien définis, qui se met en place pour résoudre le problème. Et selon les cas, l'accompagnement de la victime peut durer un jour, un mois ou… un an.

RÉPONSE AUX ÉVÈNEMENTS CYBER 2019

2 296
signalements

370
incidents

9
incidents majeurs

16
opérations
de cyberdéfense

« *Cela dépend principalement du type de menace* » décrypte Serge Lefranc. « *Dans le cas d'une attaque par rançongiciel, les effets sont immédiats et visibles. On se déploie immédiatement, c'est souvent plus court. Mais quand on est face à de l'espionnage, où l'attaquant se fait discret et où l'effet final recherché n'est pas connu, les choses sont plus diffuses et notre engagement plus long* ».

Il ne s'agit là que de la partie émergée de l'iceberg, car l'activité opérationelle ne se conçoit pas sans son volet préventif. Ainsi, l'efficacité de l'ANSSI est notamment rendue possible par le déploiement de dispositifs de détection d'attaques informatiques. En la matière, les mois et années à venir verront se développer une capacité de détection sur les systèmes, complétant celle orientée sur les réseaux. Cette activité contribue aussi à alimenter l'analyse de la menace conduite par la division connaissance et anticipation – ultime composante du fameux *handspinner*.

On a pris l'habitude, dans les murs et au-delà, de parler de « cyber-pompiers » pour qualifier ces équipes réactives qui partent, dans un effort commun, éteindre le feu. L'analogie avec le monde de la santé illustre encore davantage l'effort collectif : il s'agit d'abord, en prévention, de renforcer ses propres défenses immunitaires et de savoir repérer les anomalies. La détection des signes précurseurs d'une agression repose sur des capteurs fiables et la connaissance des « patients » exposés aux menaces. Lorsqu'un accident arrive, les urgentistes reçoivent l'alerte, posent un diagnostic et dispensent les premiers soins. Avant de réorienter les patients vers les services spécialistes de leur pathologie. C'est là qu'un traitement plus approfondi peut être délivré… si nécessaire, dans la durée.

Une préparation collective

Pour se préparer à d'éventuelles crises et toujours dans un souci de perfectionnement des méthodes, des exercices sont régulièrement organisés au sein de l'ANSSI, au niveau du SGDSN et au-delà,

en interministériel. Indispensables à la préparation de la réponse, ils permettent de développer et de tester les méthodes et de fluidifier les échanges. Lorsqu'un évènement survient dans la « vie réelle », la préexistence de processus et de relations interpersonnelles entre les individus mobilisés est en effet souvent déterminante. Ces exercices ont aussi et surtout la vertu de préparer les participants à la gestion du stress face à des évènements aux conséquences parfois dramatiques.

L'année 2019 a en particulier vu se réaliser l'exercice LockedShields. Organisé par le Centre d'excellence cyber de l'OTAN à Tallin, en Estonie, il s'agissait du plus grand exercice de cyberdéfense jamais effectué en situation réelle. Quelques chiffres en disent parfois plus que de longs discours : pendant six jours, ce sont plus de 1 200 experts en cyberdéfense issus de 23 nations qui ont dû faire face à plus de 2 500 cyberattaques. Belle preuve de l'efficacité de la coopération française : représentée par des équipes de l'ANSSI et du COMCYBER du ministère des Armées, la France est arrivée sur la plus haute marche du podium.

Enfin, dans sa dynamique d'ouverture, l'ANSSI a renforcé en 2019 sa coopération avec ses partenaires dans le cadre de la réaction aux attaques cyber. Mis en place conformément à la revue stratégique de cyberdéfense de 2018, le centre de coordination des crises cyber (C4) a intensifié son activité. Présidé par la SGDSN et se réunissant mensuellement, le niveau stratégique (C4 STRAT) définit et propose aux autorités les réponses adaptées. Au niveau technico-opérationnel, le C4 TECHOPS permet de partager l'analyse de la menace par des échanges techniques au quotidien.

Autre fait notable : l'ANSSI apporte plus que jamais à la justice une connaissance des faits et une expertise technique utiles à la conduite d'enquêtes judiciaires (voir témoignage ci-contre). Une coopération essentielle d'un côté comme de l'autre, puisqu'elle permet également à l'agence de développer sa connaissance de la menace… et de gagner, encore une fois, en efficacité. ●

ALICE CHÉRIF

Cheffe de la section cyber/J3 au parquet de Paris

« Il faut casser le sentiment d'impunité des attaquants. »

Longtemps dirigée vers les particuliers, la cybercriminalité touche désormais tous les acteurs de la société, comme ont pu le démontrer les vagues d'attaques NotPetya et Wannacry en 2017. Plus récemment, les attaques par rançongiciels ont considérablement évolué pour nous placer aujourd'hui devant des attaques délibérément orientées vers les entreprises et les institutions.
En parallèle de l'évolution de ces phénomènes, le sujet a pris une autre dimension au parquet de Paris. Alors que la question était initialement traitée au sein de la section financière, une section « cyber » indépendante a été créée. Et depuis 2016, le parquet dispose d'une compétence concurrente nationale qui vient compléter son assise parisienne. Ce changement nous confère une vision bien plus complète des enjeux. Car si chaque victime doit être considérée individuellement, le préjudice se mesure aussi à la lumière de l'ampleur de l'impact. Un seul attaquant fait parfois des milliers de victimes !
Fort heureusement, les magistrats se spécialisent sur la question. Et la justice se met en ordre de bataille avec les services d'enquête et les partenaires institutionnels comme l'ANSSI et le dispositif Cybermalveillance.gouv.fr. Aujourd'hui, les faits que l'ANSSI porte à notre connaissance nous permettent de gagner en réactivité. Par ailleurs, son accompagnement sur le plan technique nous est précieux pour mener nos enquêtes de façon plus efficace.
Il faut enfin rappeler aux victimes l'importance du dépôt de plainte. L'objectif, c'est d'aboutir à des identifications, des interpellations et des condamnations. Le tribunal correctionnel est amené à prononcer des sanctions parfois sévères – jusqu'à quinze ans de prison. Il faut aussi que les pirates aient conscience qu'en la matière, il n'y a pas d'impunité. ●

Regards croisés sur les technologies et les usages

Notre société vit au rythme de transformations numériques qui sont parfois à l'origine de ruptures profondes. L'apparition à plusieurs vitesses de nouveaux besoins, usages et technologies nous propulse vers des horizons dont les promesses enthousiasment et interrogent à la fois. Éclairer et accompagner ces (r)évolutions doivent demeurer des préoccupations de tous les instants pour l'ANSSI, qui ne saurait les aborder seule.

Celles et ceux qui ont connu l'ANSSI des débuts le savent : l'agence s'est construite sur une expertise technique et scientifique, elle-même issue d'un héritage cryptographique plus lointain encore. Dix ans plus tard, cette expertise continue d'irriguer les travaux de l'agence et investit de nouveaux terrains, dans le souci permanent de se maintenir à l'état de l'art. À la faveur des liens tissés avec des acteurs clés, l'agence contribue également à créer les espaces de dialogue dont le tissu académique national a besoin et prend une part active dans les programmes de recherche français et européens. Parce que son avis est attendu sur une variété de sujets, l'ANSSI souhaite faire entendre une voix plus prospective et la confronter à d'autres.

Recherche et innovation : l'élan européen

Grâce à ses travaux de recherche, sa propension à innover, à transmettre (formation, doctrine, publications, conférences, etc.) et sa participation active aux travaux européens (voir pp. 18-23), l'expertise de l'ANSSI rayonne bien au-delà de nos frontières. L'agence s'est ainsi naturellement engagée pour une durée de trois ans, aux côtés d'acteurs issus de 14 États membres, dans le développement d'un nouveau réseau de compétences européen en matière de recherche et d'innovation : SPARTA.

Piloté par le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) et soutenu par le programme européen Horizon 2020, le consortium SPARTA a débuté ses travaux en février 2019 et compte – outre l'ANSSI – Inria, l'Institut Mines-Télécom, Thales et YesWeHack parmi ses membres français. L'objectif de SPARTA est de ré-imaginer la manière dont la recherche, l'innovation et la formation se pratiquent et se coordonnent au sein de l'Union européenne afin de participer au renforcement de l'autonomie stratégique européenne par la mutualisation des expertises. À terme, ces travaux alimenteront également les réflexions préalables à l'établissement d'un Centre de compétences européen en cybersécurité.

47
publications scientifiques

6
thèses en cours dans des domaines aussi variés que la sécurité physique des SoC ou la détection de compromissions dans des journaux d'évènements

11
projets de recherche menés en partenariat

L'ANSSI a par ailleurs participé de 2017 à 2020 au consortium REASSURE du programme H2020 qui réunissait les universités de Louvain (Belgique) et de Bristol (Royaume-Uni), Riscure (Pays-Bas), IDEMIA (France) et NXP (Allemagne). Le but du projet était d'améliorer l'efficacité et la qualité de la certification des composants. Pour l'agence, cela a principalement été l'occasion de développer des méthodologies d'analyse basées sur des algorithmes d'apprentissage automatique. Afin d'améliorer la synergie avec la recherche académique dans ce domaine, l'agence a déposé en source ouverte sur GitHub une implémentation d'un AES (standard de chiffrement symétrique) sécurisé à l'état de l'art, les ensembles de traces enregistrées lors de son exécution et les paramètres des réseaux de neurones utilisés pour les analyser. Cette approche a pour objectif de faciliter la reproductibilité et la comparaison des résultats.

Conseil scientifique : une mobilisation des chercheurs au service de l'intérêt commun

S'il n'est pas nouveau pour les experts de l'ANSSI d'inviter leurs pairs à s'exprimer sur leurs travaux, se doter d'une instance dont

« Dans ce contexte d'accélération technologique et dans la continuité de la création d'un conseil scientifique, il s'agit de renforcer notre capacité à anticiper les ruptures technologiques et les révolutions d'usages. »

MANIFESTE DE L'ANSSI

c'est précisément la mission vis-à-vis des activités de recherche de l'agence l'est un peu plus. C'est chose faite avec la création, en février 2019, d'un conseil scientifique composé de 12 personnalités scientifiques issues du monde académique et de l'administration. Présidé par Gildas Avoine (voir Rapport annuel 2018), professeur à l'INSA Rennes, le conseil scientifique s'est réuni deux fois en 2019 et a remis à l'ANSSI ses premières conclusions en janvier 2020.

En s'appuyant sur leur connaissance de l'activité scientifique de l'agence et des échanges fréquents avec ses représentants, les membres de ce conseil ont émis une dizaine de recommandations à son endroit. Ainsi, l'accent a été mis sur l'importance des projets transverses menés par les sept laboratoires de la division Scientifique et technique. Citons par exemple les projets WooKey (voir Rapport annuel 2018) et Playmobile. Ce dernier est né du souhait de l'ANSSI de monter en compétence dans le domaine de la sécurité des plates-formes mobiles, en particulier dans celui des architectures sécurisées basées sur des *System on Chip* (SoC). Pour accompagner la réflexion prospective de l'agence, le conseil propose par ailleurs de contribuer à la mise à jour de sa feuille de route technologique. L'expérience de ses membres sera également très appréciée dans le cadre du partenariat renforcé entre l'ANSSI et Inria aujourd'hui, et demain

Conseil scientifique
De gauche à droite : Vincent Strubel, Emmanuel Germain, Éric Freyssinet, Frédéric Valette, Guillaume Poupard, Véronique Cortier, Jean-Yves Marion, David Pointcheval, Henri Verdier, Hervé Debar, Gildas Avoine, Aurélien Francillon, Catuscia Palamidessi, François-Xavier Standaert, Claude Kirchner, Geoffroy Hermann

avec d'autres acteurs académiques. Un objectif qui va de pair avec celui de mieux communiquer sur l'implication de l'agence dans le monde de la recherche, qu'il s'agisse de projets ou d'instances de gouvernance. En 2019 par exemple, l'agence s'est impliquée dans 11 projets : trois soutenus par l'Agence nationale de la recherche, cinq issus de pôles de compétitivité nationaux, deux dans le cadre du programme européen H2020 et un en matière de cryptographie post-quantique qui relève des investissements d'avenir. L'ANSSI rejoint enfin l'avis du conseil dans sa volonté d'accroître ses relations avec les universités et écoles. Le partenariat avec Inria ou encore la création d'un futur Campus Cyber (voir p.17) pourront favoriser le développement de cet axe.

Conjuguer recherche académique et réalité opérationnelle

Les directions générales d'Inria et de l'ANSSI ont récemment donné un nouvel élan à leur coopération en l'inscrivant dans leurs orientations stratégiques respectives. Pour l'agence, cette démarche prouve une nouvelle fois son souhait de co-construire avec l'écosystème national. L'objet de cette coopération est de définir un partenariat mutuellement bénéfique du point de vue scientifique et technique et de préfigurer les modalités de coopération qui pourraient à terme être étendues à d'autres partenaires de l'agence. ●

BRUNO SPORTISSE

Président-directeur général d'Inria

« Construire ensemble la confiance et la souveraineté numériques. »

Le développement des usages et technologies numériques repose sur la capacité de tout un écosystème à y apporter des garanties de confiance. La cybersécurité se situe donc naturellement au cœur de l'activité d'Inria. S'il est essentiel de faire entendre notre voix sur les enjeux de la transformation numérique, il est crucial de ne pas nous exprimer seuls. Derrière les *buzzwords* (IA en tête) se cache une réalité scientifique et technologique mais les autres dimensions sont tout aussi importantes ! Depuis près de dix ans, nous collaborons ainsi avec l'ANSSI et je suis convaincu que allons passer à la vitesse supérieure. Pour l'institut, ce partenariat constitue une réelle opportunité de considérer les problèmes « à l'échelle » en accédant à des données ainsi qu'à des réalités opérationnelles sur un sujet critique. Les enjeux du numérique sont à présent bien perceptibles par tous, avec leurs dimensions sociales, économiques et politiques. Construire notre souveraineté numérique, l'ambition d'Inria pour 2023, passe par un partenariat renforcé avec l'ANSSI et nous en faisons l'une de nos priorités stratégiques. Cela doit aussi s'incarner par des formes renouvelées et audacieuses de partenariat : nos deux organisations doivent prendre le risque d'innover pour construire la confiance numérique, au service de l'État et de notre pays. ●

En 2018, l'ANSSI avait entrepris des travaux internes pour porter une vision prospective sur des technologies et usages de rupture. Dans la continuité des réflexions issues de ce groupe de travail, l'objectif est désormais d'aller plus loin en jouant à plein notre rôle d'éclaireurs avec ceux qui nous entourent. Les cinq sujets qui suivent nous amènent ainsi à exprimer notre vision des choses et aussi à nous poser, collectivement, les bonnes questions.

« Le recours à l'expertise académique, y compris aux sciences humaines et sociales, doit nous permettre de renforcer nos messages et d'élargir nos capacités d'influence. »

MANIFESTE DE L'ANSSI

INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle (IA) n'est pas qu'un *buzzword*, elle est l'une des technologies les plus transformatrices de notre époque. Elle n'est pas non plus une fin en soi, mais un moyen, parmi d'autres, de répondre à de nombreux défis sociétaux. Aujourd'hui, favoriser le développement de systèmes d'IA « dignes de confiance » suppose de saisir les impacts de l'IA sur la sécurité numérique et inversement. Des enjeux dont le gouvernement entend s'emparer avec le lancement de Grands défis technologiques présentant des impacts scientifiques, sociaux et économiques certains.

L'IA fait l'objet d'une stratégie de la Commission européenne qui positionne l'humain au cœur. Dans ce cadre, elle a créé un groupe de 52 experts de haut niveau sur l'intelligence artificielle (AI HLEG) auquel je participe. Ensemble, nous émettons des recommandations en matière d'éthique, de politique publique et d'investissement. Nous appelons à ce que les systèmes d'IA soient « dignes de confiance », c'est-à-dire légaux, éthiques et robustes. Mais pour cela, il est urgent d'agir sur quatre leviers que sont les données, l'éducation, la réglementation et les investissements. En procédant à l'analyse des risques induits par ces usages, différents types de menaces se dégagent, à l'image de « l'empoisonnement de données » (modification des données durant l'apprentissage), du *model evasion* (déviation par rapport à ce que le modèle est supposé faire) ou du *model inversion* (extraction de certaines données secrètes du modèle). Demain, le Campus Cyber constituera pour l'écosystème une véritable plateforme d'expérimentation sur ces enjeux tandis que les grands défis IA du gouvernement vont permettre de favoriser l'innovation de rupture. Nous avons tous un rôle à jouer pour maximiser l'utilisation de l'IA en minimisant ses risques. C'est la condition d'une IA digne de confiance. ●

YANN BONNET
Directeur de cabinet, ANSSI

Mon grand défi consiste à faire émerger des innovations de rupture et une dynamique de l'écosystème en faveur de l'automatisation de la cybersécurité. Ceci afin d'absorber plus de données, de mieux les valoriser ou de rendre la cybersécurité accessible au plus grand nombre, en veillant à ce que le traitement soit transparent pour l'utilisateur. L'idée d'appliquer de l'IA à la cyber-sécurité existe déjà depuis quelques années et la popularité croissante de l'apprentissage machine l'a largement favorisée. Cet enjeu d'automatisation présente un intérêt à la fois en amont (évaluation, maîtrise du risque), en détection et en aval (remédiation) pour tout l'écosystème : chercheurs, utilisateurs, éditeurs de solutions, etc. Le grand défi doit permettre des financements importants sur des aspects qu'il est difficile de faire porter par les seuls acteurs privés (risque technique important, horizon long terme, etc.). Cela constitue un levier important pour notre économie et plusieurs sujets technologiques et sociétaux y seront abordés (données, IoT, cybercriminalité, etc.). À l'image d'autres domaines traitants de sécurité, l'automatisation de la cybersécurité doit, au bon niveau, fournir les solutions nécessaires à l'humain qui restera au centre de cette problématique. ●

WILLIAM LECAT
Directeur du Grand défi « Automatisation de la cybersécurité »

Le grand défi que je dirige sur les systèmes à base d'intelligence artificielle comporte un double enjeu. Il s'agit non seulement de garantir la sécurité et la sûreté de fonctionnement de ces systèmes – particulièrement dans les domaines critiques –, mais également d'en démontrer le caractère explicable. La confiance placée dans ces solutions est donc au cœur de mes préoccupations et doit impérativement être développée. Le déploiement de l'IA est réel et porteur de grandes promesses. Or de la preuve de concept au produit, il convient de disposer des solutions et technologies de rupture garantissant cette confiance, élément clé d'acceptabilité sociale pour tous. C'est l'objet des trois axes stratégiques de la feuille de route du programme : environnement pour la sûreté et la sécurité dès la conception ; évaluation et validation fonctionnelle du système applicatif ; normalisation et IA. Dans un enjeu de souveraineté nationale et alors que la compétition internationale a commencé, il s'agit de conférer un avantage compétitif aux acteurs français et de répondre aux attentes des citoyens. L'écosystème national est bien positionné pour relever ce challenge qui intéresse l'industrie, l'État et est l'un des piliers de la mission Villani. ●

JULIEN CHIARONI
Directeur du Grand défi « Comment sécuriser, certifier et fiabiliser les systèmes ayant recours à l'intelligence artificielle ? »

IDENTITÉ NUMÉRIQUE

L'identité numérique représente l'identité du citoyen dans l'espace numérique. Alors que les transactions électroniques se multiplient, elle apporte la preuve de son identité pour accéder à un service donné (impôts, assurance maladie, achats en ligne, etc.). Mais ce développement reste limité en l'absence d'une identité numérique hautement sécurisée. Le déploiement en France d'une identité numérique de confiance conforme aux exigences européennes et capable de faciliter et sécuriser à la fois l'accès à ces services est donc fortement attendu.

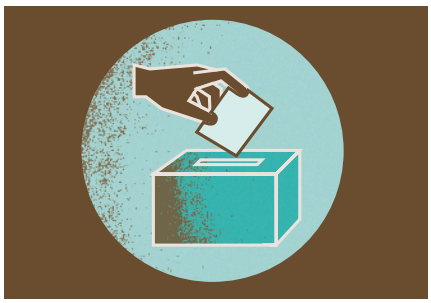
J'ai eu, au cours de ma carrière d'inspectrice générale de l'administration, l'occasion d'accompagner diverses réformes et transformations interministérielles. En 2018, les ministres de l'Intérieur, de la Justice et le secrétaire d'État en charge du Numérique m'ont nommée directrice du programme « France Identité Numérique ». L'objet de ce programme d'État est de permettre aux citoyens d'être en capacité de prouver leur identité de manière simple, mais très sécurisée dans le monde numérique comme dans le monde physique à partir des titres d'identité dotés d'un composant électronique (passeports, titres de séjour…) et, à partir de l'été 2021, d'une nouvelle carte d'identité. Tout comme cette dernière, l'identité numérique garantie par l'État sera gratuite et facultative. Et comme tout service public, elle vise l'universalité et l'accessibilité de tous les usagers. Les enjeux du programme sont donc multiples : robustesse technique, ergonomie, souveraineté, déploiement de confiance et inclusion. C'est pourquoi il associe un très grand nombre d'acteurs, publics et privés, sous le regard vigilant et le contrôle de l'ANSSI et de la CNIL. Dans notre environnement de plus en plus dématérialisé, l'identité numérique ne résout pas tout, mais elle est la porte d'accès aux droits et services et la garantie de la maîtrise par chacune de ses données les plus sensibles, la condition d'une réelle citoyenneté numérique. ●

VALÉRIE PENEAU
Directrice du programme interministériel
France Identité Numérique

En 2016, l'agence m'a nommé chef du projet de mise en œuvre du réglement européen « eIDAS » portant sur l'identification électronique et les services de confiance et dont l'objectif est d'accroitre la confiance dans les transactions électroniques au sein de l'UE. Pour l'ANSSI, cela visait notamment à établir, sur la base de critères européens, un socle commun d'exigences de sécurité pour les identités numériques nationales déployées. Depuis, l'agence accompagne des acteurs publics français dans leurs travaux liés à l'identité numérique et participe aux instances de coopération européennes mises en place. Elle a ainsi pu apporter son assistance au programme « France Identité Numérique ». L'objectif est d'assurer une meilleure prise en compte des exigences de sécurité sans freiner l'innovation, en vue de présenter aux citoyens un parcours d'identifiation numérique sécurisé et ergonomique. En effet, les technologies évoluent, l'environnement mobile devient progressivement le centre de gravité des transactions électroniques, et les moyens mis à disposition du citoyen doivent tenir compte de cette réalité. Il est ainsi impératif de prendre en compte ce nouveau contexte dans une démarche de gestion de risques adaptée, permettant de lutter efficacement contre les risques d'usurpation et d'altération de l'identité, en particulier pour les cas d'usage les plus sensibles. Cela implique notamment d'apporter des garanties à chaque étape du cycle de vie d'une identité numérique (vérification initiale de l'identité, délivrance, activation, utilisation, révocation). La résilience de l'ensemble du système est également prioritaire puisqu'aucune technologie n'est infaillible. Aussi, lorsque l'identité numérique aura fait son entrée dans le quotidien des Français, garantir la continuité des services proposés constituera l'une des conditions de son succès. ●

ROMAIN SANTINI
Chef du bureau Ingénierie
du cadre réglementaire et normatif, ANSSI

VOTE ÉLECTRONIQUE



Le vote électronique désigne selon les cas le recours à un système de vote par Internet ou à une machine à voter. Nous parlons ici de vote par Internet, que les français de l'étranger peuvent mettre en œuvre depuis 2012 dans le cadre des scrutins législatif et consulaire. Ce vote électronique évolue au gré des technologies et de l'état de la menace. Sans jamais égaler les propriétés d'un scrutin traditionnel, qui assure sincérité et anonymat du vote d'une manière compréhensible par tous, il constitue néanmoins une alternative interessante.

En juillet 2019, j'ai pris la tête de la direction des Français de l'étranger et de l'administration consulaire. Une institution que je connais bien pour y avoir été directrice adjointe et cheffe du service des Français de l'étranger (2013-2016). J'ai donc pu accompagner les déploiements du vote par Internet pour les Français de l'étranger, leur donnant ainsi accès à un exercice citoyen absolument essentiel. Pour les élections législatives de 2017 et en dépit des efforts fournis pour apporter toutes les garanties de confiance, la solution ne fut pas jugée suffisamment robuste au regard de la menace observée et nous avons donc renoncé à sa mise en œuvre. Un an plus tard, le président de la République s'engageait à rendre possible le vote par Internet pour les Français de l'étranger pour les prochaines élections consulaires et législatives. Nous avons donc travaillé avec nos partenaires (ANSSI, CNIL, ministère de l'Intérieur, etc.) pour faire évoluer la solution dans la perspective des élections consulaires de 2020. Testée à grande échelle à deux reprises et notamment en situation de crise, la solution a été homologuée en janvier. Bien qu'il s'agisse d'une procédure dématérialisée, l'objectif reste d'aller au plus près des conditions de vote traditionnelles en apportant aux électeurs confiance dans la solution et facilité d'accès. ●

LAURENCE HAGUENAUER
Directrice des Français de l'étranger et de l'administration consulaire, ministère de l'Europe et des Affaires étrangères

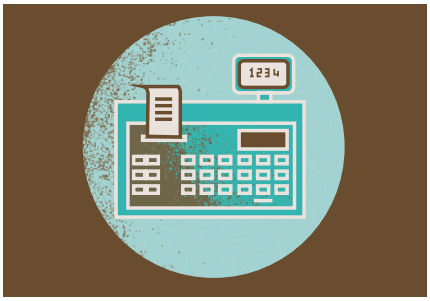
L'implication de l'ANSSI sur le vote électronique n'est pas nouvelle mais sa nature est assez inhabituelle. L'accompagnement « classique » de l'agence (assistance technique, audits, aide à l'homologation, etc.) se double ici d'une participation au bureau de vote électronique. Ce dernier réunit un président membre du Conseil d'État, des représentants élus des français de l'étranger, et des agents des ministères de l'Europe et des Affaires étrangères, de l'Intérieur, et de l'ANSSI. Il veille à garantir la confiance dans le scrutin en conciliant les enjeux de transparence vis-à-vis des électeurs et de sécurité du système. En tant que sous-directeur Expertise, j'y ai représenté l'agence en 2017 et 2020 pour y partager notamment des éléments d'appréciation de la menace. À l'approche des législatives de 2017, celle-ci était accrue et s'en prémunir nécessitait de renforcer significativement la sécurité du système en temps très contraints. En s'appuyant sur un processus collégial incluant le bureau de vote électronique, l'exécutif a donc décidé d'y renoncer. Depuis, nous sommes tournés vers les consulaires de 2020 et nous avons pu apporter au système de vote les garanties de confiance attendues et l'éprouver lors de tests grandeur nature. ●

VINCENT STRUBEL
Sous-directeur Expertise, ANSSI

Au début des années 2000, le vote électronique est devenu un sujet à la mode. En la matière, le parallèle fait entre les propriétés du vote papier et celles du vote électronique constitue le point de départ de nombreuses réflexions. D'un point de vue purement académique, on considère le problème résolu puisque des procédés cryptographiques permettent d'aboutir à un « vote universellement vérifiable ». Cela signifie que chaque étape du scrutin est vérifiable par et pour tout le monde. Mais si l'homme de l'art le comprend, comment assurer aux citoyennes et citoyens qu'ils s'expriment secrètement et qu'en même temps, il est possible de vérifier chaque étape du scrutin ? C'est là tout le paradoxe ! Conséquence directe, on passe 80 % de notre temps non pas sur la cryptographie mais sur l'identification car, « dans la vraie vie », les votants n'ont pas de clé publique pour s'identifier. D'autres moyens sont donc développés or, plus on apporte de moyens de vérification aux votants, plus on s'expose aux suspicions et on alourdit le système. Si l'on dispose un jour d'un titre d'identité numérique, cela règlerait une partie significative du problème. ●

DAVID POINTCHEVAL
Directeur du département d'informatique de l'ENS et membre du conseil scientifique de l'ANSSI

BLOCKCHAIN



La *blockchain*, popularisée par la crypto-monnaie Bitcoin, est une technologie permettant à un ensemble d'acteurs de réaliser des transactions selon un mode de gestion collaborative. En se passant de tiers de confiance, la progression de cet usage fait naître diverses interrogations sur ses applications possibles, la cybersécurité, l'identité des contributeurs et la pérennité même de cette solution.

Les *blockchains* dites « ouvertes » sont aujourd'hui les plus connues. Leur sécurité repose sur un principe de « consensus » qui permet aux acteurs honnêtes de contrôler la chaîne s'ils possèdent la majorité de la puissance de calcul. L'évolution future de cette puissance et de sa répartition est difficile à évaluer. Dans les *blockchains* « fermées », ne contribue pas qui veut. Cela constitue un gage de sécurité, mais ce fonctionnement les apparente à des bases de données distribuées classiques. Si elles peuvent trouver leurs usages, comment garantir la véracité des informations qui s'y trouvent ? ●

SÉBASTIEN KUNZ-JACQUES
Chef adjoint de la division Scientifique et technique

ALGORITHMES DE CRYPTOGRAPHIE POST-QUANTIQUE

En cryptologie, on part de l'hypothèse que l'on ne connaît pas les capacités de l'adversaire. On lui prête donc, par prudence, des capacités qu'il n'a peut-être pas. C'est ce qui se passe pour l'éventuelle apparition d'un ordinateur quantique universel. La question n'est pas de savoir si une telle machine a des chances de voir le jour, mais bien de ne pas ignorer cette possibilité et de s'y préparer.

Anticiper l'arrivée possible de l'ordinateur quantique universel nous place devant le défi de mettre au point de nouvelles méthodes de protection des communications dites *quantum-safe*, résistant aux attaques d'une telle machine. La communauté académique internationale se mobilise dans cet objectif, notamment dans le cadre de la compétition organisée par le NIST. S'il faudra plusieurs années à ces nouveaux mécanismes pour atteindre un niveau de maturité comparable aux algorithmes actuels, nous pensons à l'ANSSI que dans l'intérim, la bonne voie consiste en la combinaison de mécanismes éprouvés avec les candidats *quantum-safe*. ●

SÉBASTIEN KUNZ-JACQUES
Chef adjoint de la division Scientifique et technique

ANSSI in action: looking back on 2019

From the celebration of its 10th anniversary to the success of the first edition of Blue OLEx, the European Union (EU)'s new cyber crisis management framework, 2019 has been a particularly rich and intense year for the French National Cybersecurity Agency (ANSSI). This review provides an insight into ANSSI's role, as a leader and technical adviser to ministerial partners; to better understand and respond to cyber threats, to educate and raise younger generations' awareness of digital risks, to contribute to European sovereignty, and to strengthen stability in cyberspace.

To celebrate the important milestone of its 10th anniversary in 2019, ANSSI organised a one-off Cyber Festival in June, which brought together the main stakeholders of the French cyber security ecosystem. In addition to looking back over ten years of ANSSI action, this festive and open event also gave participants the opportunity to further discuss the role of ANSSI in the coming years, and better ways to build tomorrow's digital trust, together.

The collaborative reflection of the Cyber Festival had been conceived as an early stage of the broader ANSSI10+ initiative, which is designed to define the agency's new strategy, visions and priorities. After a few months of further workshops, ANSSI published its vision in its *Manifesto, for the ANSSI of the next ten years*. The new strategic directions described in the manifesto will guide ANSSI's actions for the coming years.

European cooperation

ANSSI has always worked closely with counterparts around the world to secure cyber space. In the past year, the agency has been more involved than ever at the EU level, in coordination with its European partners, such as Germany and the Netherlands (see interview with Patricia Zorko, available in French, p. 23). Its contribution to promoting European sovereignty and its commitment to strengthening cybersecurity within EU institutions are substantial.

CYBERSECURITY ACT

On 7 June 2019, the Council of Europe adopted the European Cybersecurity Act. This regulation, which is a real step forward for European strategic autonomy, has two main objectives: firstly, it grants a permanent mandate to the EU Cybersecurity Agency (ENISA), more resources and new tasks; and secondly, it creates a European cybersecurity certification framework, essential to reinforce the security of the European digital single market.

The Cybersecurity Act had been the subject of intense negotiations since 2017. Thanks to its expertise in certifying security products and services, ANSSI contributed significantly to the adoption of this new regulation in 2019.

> **"Cyber Festival was a day which embodied my vision for the agency."**
>
> GUILLAUME POUPARD
> *Director-General of ANSSI*

CYBERSECURITY OF FIFTH GENERATION NETWORKS

Fifth Generation (5G) networks are cutting-edge wireless technologies. They will do more than simply offer faster communications: in our increasingly integrated digitised economies and societies, many critical sectors will be significantly impacted, including transport, energy, and health. Ensuring the security of 5G networks is therefore essential. EU member states have identified security challenges associated with this innovative technology.
In 2019, ANSSI was particularly involved in the European works, which consisted of a EU-coordinated 5G networks risk assessment and threat analysis. Those formative works led to the development of the EU 5G Toolbox on Cybersecurity, which was launched in January 2020. This joint toolbox, which is a set of mitigation measures designed to help EU member states address security risks related to the roll-out of 5G, contributes significantly to European sovereignty.

"We are very happy that we can continue this tradition established by our French friends and organise the next edition of Blue OLEx."

PATRICIA ZORKO
Deputy National Coordinator for Security and Counter-terrorism, The Netherlands

BLUE OLEx 2019

In 2017, the European Commission adopted a recommendation regarding the operational level of the European cyber crisis response framework, also known as Blueprint. This recommendation proposed that EU member states and relevant European institutions agree on European cooperation and exchange procedures for the management of major incidents and cyber crises. Three levels of crisis management were identified: political, operational, and technical.

These resolutions led France and Spain, supported by many EU member states, to establish Blue OLEx. This new joint initiative, set up as part of the Network of Information Security Directive (NIS) Cooperation Group, was designed to bring together the main stakeholders for a high-level cyber crisis exercise. France hosted the first edition of Blue OLEx on 2 and 3 June 2019. The operational level of the EU cyber crisis framework, represented by heads of the national cybersecurity authorities of 23 EU member states, ENISA and the European Commission, gathered in Paris for a table-top exercise. Besides identifying our strengths, weaknesses and areas of improvement in a cyber-related crisis situation, this high-level gathering has shown that, in the area of cybersecurity, voluntary cooperation amongst countries and anticipation are critical. In 2020, the second edition of Blue OLEx is organised by the Netherlands.

CSIRTS NETWORK

Cooperation amongst the members of the CSIRTs network has soared in maturity with the organisation by ENISA, in May 2019, of the CSIRTs Network's second excercise, CyberSOPEx2019. The objective of this cyber exercise was to test cooperation between the network members during large-scale attacks. Once again, it proved that the high levels of trust and cooperation that exist between the countries are crucial in addressing such attacks.

"CYBERMOI/S" AND THE EUROPEAN CYBERSECURITY CHALLENGE

For several years, France has been taking part in the European Cybersecurity Month (ECSM), the EU's annual awareness campaign coordinated by ENISA in October. In France, the campain is led by ANSSI, which in 2019 chose to name it "Cybermoi/s". During the whole month, administrations, associations and stakeholders involved in raising awareness of cybersecurity organised events and activities across the country in order to help citizens understand cybersecurity issues.

As part of ECSM, ENISA also coordinated the European Cybersecurity Challenge (ECSC). This initiative was designed to enhance cybersecurity talent in Europe and connect high-potential individuals with industry-leading organisations. The fourth edition of ECSC took place in Bucharest (Romania) in 2019. This was the second time that Team France took part, and the team – led by ANSSI once again and composed of 10 players between the ages of 17 and 25 – had been well trained and mentored beforehand. In 2020, ANSSI will again participate in these two European initiatives which contribute so much to promote European values.

DIGITAL RISK MANAGEMENT

In the coming years, ANSSI participated, for the first time, in the FERMA Forum, the European Risk Management Forum which took place in Berlin. In partnership with the French Association for Corporate Risks and Insurance Management (AMRAE), ANSSI launched at FERMA a 15-step guide to help managers of private and public organisations of all sizes in the building of a digital risk management policy. With this guide, France strives to share its experiences and expertise

in digital risk management at the European level. ANSSI and AMRAE plead for sharing common principles that will facilitate the coordination of EU member states faced with current and future threats.

International cooperation

Internationally, ANSSI actively promotes peace and stability in cyber space, as these values are key concerns of the agency and its ministerial partners. Knowledge of threat is also shared with trusted partners. Trust and cooperation are not catchwords, they are commitments which sometimes go beyond information sharing and lead to joint cyberdefence operations.

PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE

On 18 November 2018, during the Internet Governance Forum held at UNESCO and the Paris Peace Forum, President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace. This Call invited states, organisations, civil society, and private stakeholders to mobilise for peace, stability, and security in cyber space. This initiative, supported by over 500 entities, is based on nine principles – including the protection of individuals and insfrastructure, protection of the Internet, and the defence of intellectual property – , which ANSSI has worked continuously to promote across the world. In line with the Paris Call, the Organisation for Economic Co-operation and ➔

"I strive to instill a virtuous cycle of trust with our peers and our main partners: we are stronger together."

SAÂD KADHI
Head of Cert-EU

Representatives of EU member states gathered in Paris for the first edition of Blue OLEx.

OPERATIONAL FIGURES *

2,296
reports

370
incidents

9
major incidents

16
cyberdefence operations

* *Number of interventions carried out by ANSSI in 2019.*

➲ Development (OECD) held the Global Forum on Digital Security for Prosperity in November 2019. Henri Verdier, French Ambassador for Digital Affairs, and Guillaume Poupard, Director-General of ANSSI, took part in this event and presented the French vision for putting an end to the development of a "digital Far West". Alongside the French Ministry for Europe and Foreign Affairs, ANSSI, leveraging its expertise, plays a crucial role in the promotion and implementation of the Paris Call principles and values.

Threat analysis

By its very nature, ANSSI is open to the cybersecurity ecosystem. To fulfill its vision, the agency, through CERT-FR, publishes analysis reports, both in French and in English. In 2019, ANSSI continued to share its expertise and developed partnerships with French administrations beyond this ecosystem. These partnerships enable the agency to deepen its knowledge of threat and to be both more resilient and more efficient. In 2019, three trends have been observed by ANSSI Operations Department in the cyber threat landscape.

• Ransomware: the number of ransomware attacks was particularly high in 2019. They were aimed at both companies and public organisations. These attacks can have serious consequences on information systems and have a long-lasting impact. Health, media, food industry... No sector is spared.

• Espionage: in 2019, espionage operations continued on an upward trend. For attackers, the main motivations are the search for strategic information, foreign and defence policies, access to industrial information and trade secrets of organisations, and theft of personal data.

• Supply chain attack: these attacks increased considerably in 2019. They consist of taking advantage of trusting relationships between partners. Cybercriminals infiltrate the organisations or companies systems through their providers (digital service companies, service providers, Internet, outsourcing companies, etc.).

INTER-MINISTERIAL COOPERATION

Following the Strategic Review of Cyberdefence, a Cyber Crisis Coordination Centre (C4) was established in 2018. C4 was particularly dynamic in 2019. This inter-ministerial mechanism for threat analysis, preparedness, and coordination was designed to bring together all of the concerned stakeholders. It is composed of two levels:

- strategic (C4 STRAT). Presided over by the Secretary-General for Defence and National Security, C4 STRAT is in charge of facilitating the preparation of the State's response options and strengthening France's position internationally.
- technical-operational (C4 TECHOPS). The mission of C4 TECHOPS is to ensure information sharing.

JUDICIAL COOPERATION

In 2019, ANSSI worked closely with the Paris Public Prosecutor's office in which a cyber unit has been established. Since 2016, the Paris Public Prosecutor has had national powers regarding cybercrime. Thanks to ANSSI's expertise, it is more responsive and more efficient in its investigations. The well-known cyber attack NotPetya was the turning point in cooperation between the two administrations. This case is still under investigation at an international level. Within the framework of this investigation, ANSSI supports the Paris Public Prosecutor in its collaboration with the EU Agency for Criminal Justice Cooperation (EUROJUST).

Human values

ANSSI is a dynamic and agile organisation, thanks to its wide range of profiles and expertise. Openness, agility and internally-shared skills are core values within the agency, which continues to engage more and more new discussions and partnerships. While openness beyond the ecosystem is important, listening ➔

HENRI VERDIER

French Ambassador for Digital Affairs

"France is fully committed to advocating for a free, neutral, open, secure, and unique digital space."

Thanks to its principles of openness, transparency and cooperation, the digital revolution has been the greatest accelerator of economic, social and democratic innovation in history. The Internet is undoubtedly one of the greatest innovations the world has ever seen. Nowadays, however, for various reasons – cybercrime, propaganda, manipulation of information, etc. – many stakeholders are trying to use it as a tool to weaken our democracies.
France has always been dedicated to protecting fundamental rights, access to knowledge and culture, and fostering artistic and cultural creation. French digital diplomacy is based on five issues: technological innovation; security (cybersecurity and protection against harmful content); Internet governance; economic diplomacy; and promotion of our democratic values.
Our vision is clear: we are fully commited to advocating for a free, neutral, open, secure, and unique digital space. Our fellow citizens should, at a minimum, have access to basic technologies and secure social media without being exposed to hate. As French Ambassador for Digital Affairs, my mission is to promote this vision across the world: in multilateral fora, and in bilateral dialogues. The French Ministry for Europe and Foreign Affairs provide all diplomatic means available to support this.
France has also launched new initiatives such as the Christchurch Call, or the Paris Call for Trust and Security in Cyberspace. This Call, aimed at promoting peace and stability in cyber space, has been drafted hand in hand with ANSSI, which is a valuable partner in all cybersecurity matters, including on the UN discussions on the stability of cyber space. Together, with ANSSI, we are fully dedicated to promoting France's vision in Europe, and around the world. ●

and disseminating knowledge are even more so: to strengthen these, ANSSI launched or took part in several initiatives during 2019 to enable passing on skills and knowledge, listening, and sharing.

PASSING ON

In our increasingly digitalised economies and societies, raising younger generations' awareness of digital risks is crucial. ANSSI is firmly committed to strenghtening cybersecurity instruction from the earliest age, and to nurturing vocations. ANSSI, in partnership with the French Ministry for Education and Youth, has designed a roadmap to fulfil these commitments. The agency is working on the development of resources to support cybersecurity education in schools and its expertise is called upon by educational publishers. ANSSI is also involved in Service National Universel (SNU), a one-month compulsory service programme, coordinated by the Ministry of Armed Forces, for all French citizens aged 15 to 17. The agency developed a large part of the cybersecurity programme delivered as part of the SNU, which is addressed from the standpoint of best practices.

LISTENING

2019 has been a milestone for ANSSI in many fields. Besides celebrating its anniversary and taking part increasingly in international outreach, the agency opened a new chapter in scientific research and into the social effects linked to digitalisation. In February 2019, a Scientific council composing 12 leading scientists was established. The mission of this team of experts is in particular to support the agency in anticipating the major challenges in digital security, and to advise on research topics. Once again, ANSSI fulfils its vision of openness and listening. A scientific activity report detailing the projects carried out by ANSSI had been provided to the members of the scientific council and led them to make a dozen recommandations. They suggested in particular to: promote transversal projects between the seven laboratories of the scientific and technical department; update ANSSI's technology roadmap; and better communicate on the agency's active participation in research.

> **"Skills, openness and agility are ANSSI's core values. They underpin our strategy."**
>
> ANSSI's Manifesto

Agora 41 may sound like a code word, but it is actually the name of an ANSSI initiative. Agora 41 is a focus group composed of 41 members from different sectors, which was designed to initiate and feed comprehensive discussions on non-technical but digital security-related topics. The members share and develop their thoughts within five working groups: collective imagination, regulation, talents, "cyber-me", and ecosystem.

SHARING

Sharing is part of ANSSI's DNA. The agency, which is one of the French administration's biggest contributors to Open Source, has always taken part in Open Source projects and is committed to continuing in that direction. This approach facilitates knowledge and solutions sharing and ensures that ANSSI benefits from and contributes to the broader Open Source community. ANSSI's expertise and values also spread outside France.

At the European level, the agency is involved in the EU research and innovation programme, Horizon 2020, through its participation in two consortia: REASSURE and SPARTA.

REASSURE: from 2017 to 2020, this consortium, composed of stakeholders from five EU member states, was notably designed to improve the efficiency and quality of all aspects of certification; to deliver tools to stakeholders; and to improve existing standards.

SPARTA: alongside 43 stakeholders from 14 EU member states, ANSSI is involved in the development of this new European network of skills in cybersecurity research and innovation. This three-year project is led by French Alternatives Energie and the Atomic Energy Commission. Inria, Institut Mines-Télécom, Thales and YesWeHack are the main French players taking part in the consortium which has been launched in February 2019. Through a wide range of activities, SPARTA's objective is to re-imagine the way that cybersecurity research, innovation, and training are performed in Europe, both in academia and in industry. Thanks to the sharing of expertise and skills, this initiative contributes to strengthening European technological sovereignty.

GUILLAUME POUPARD

Director-General of ANSSI

The year 2019 was a milestone in many fields for ANSSI, not only nationally, but also at the European and international levels.

We are proud of what we have accomplished over the years, and we are determined to continue in the same direction. It is also a great privilege for me to work in a such dynamic environment, and with the extraordinary people who make up the agency. It is no exaggeration to say that without the exceptional levels of professionalism, expertise and dedication which these employees bring to their missions, day in and day out, we would not be in our current position of strength.

Netherless, we must remain vigilant. The path ahead is strewn with potential ambushes: current and upcoming challenges are tremendous and oblige us to be more demanding with ourselves, and to be more efficient and proactive. The years 2020 and ahead are no exception.

As our societies and economies become more and more digitalised, digital security and economic, political, and societal concerns are converging. The great advantages brought by digitalisation render all the more critical the need to adress threats that might affect it; and these threats are very real and cannot be ignored.

In Europe, considerable progress has been collectively achieved to strengthen our digital sovereignty. However, the efforts made to adopt the Cybersecurity Act and to develop the EU 5G Toolbox need to be continued. There is, of course, still much more work to be done.

With the beginning of the new European legislature, 2020 is also a challenging year for the EU: the growth of cyber threat remains a key concern for the EU institutions and the member states, and the challenges ahead show us that, more than ever, collective action, trust and cooperation amongst stakeholders play a significant role. In this context, as we strive to build a common European ambition, experience sharing and networking are crucial. Blue OLEx was a good example of high-level European cooperation on cyber issues. Together, with all European stakeholders, we have to renew our efforts in support of full European sovereignty.

It is fundamental that we reassert and promote, on the international stage, the European values which are so important to us. Peace, security, and stability of and within cyber space are not empty words, they have to be translated into action.

France is committed to promoting peace and stability in cyber space. To achieve this in what is a new and evolving field will require the establishment of new rules of responsible conduct for states, within the framework of existing international law. As part of multilateral fora, and more particularly in UN negotiations, ANSSI works continuously with all the concerned stakeholders and ministerial partners to this end. Indeed, ANSSI is deeply convinced that it is only through cooperation and coordination that we will be able to further our objective of a peaceful and stable cyber space. ●

Bibliographie 2019

Guides

- *Exigences de sécurité matérielles*, guide technique
- *Maîtrise du risque numérique – L'atout confiance,* guide, en partenariat avec l'AMRAE
- *Recommandations de sécurité relatives à un système GNU/Linux*, guide technique
- *Recommandations pour une utilisation sécurisée de Zed!*, guide technique
- *Recommandations relatives à l'interconnexion d'un système d'information à Internet*, guide technique
- *Sécurité numérique – Bonnes pratiques à l'usage des directeurs et directrices de campagne*, guide
- *Sécurité numérique – Bonnes pratiques à l'usage des participants au G7*, guide
- *Sécurité numérique – Bonnes pratiques à l'usage des professionnels en déplacement*, guide

Publications scientifiques

Division Scientifique et technique

- *IA et cybersécurité : une boucle émergente de rétroactions*, G. Hermann, Revue Défense Nationale, numéro 821, juin 2019

1.1 Laboratoire architecture matérielle et logicielle (LAM)

- *Overview of Fuchsia, a new operating system*, M. Salaün, Embedded Recipes 2019
- *Sécurité de Debian Buster*, Y.-A. Perez, MISC, numéro 102, mars 2019
- *CLIPS OS : un système d'exploitation durci open-source*, T. Ravier, Journées nationales du GDR Sécurité informatique
- *Hardware and software security research at ANSSI: two case studies*, Y.-A. Perez, SILM Workshop

1.2 Laboratoire cryptologie (LCR)

- *Aggregate Cash Systems: A Cryptographic Investigation of Mimblewimble*, G. Fuchsbauer, M. Orru, Y. Seurin, EUROCRYPT 2019, pp. 657-689
- *An Efficient and Provable Masked Implementation of qTESLA*, F. Gérard, M. Rossi, conférence CARDIS 2019
- *Assessment of the Key-Reuse Resistance of NewHope*, A. Bauer, H. Gilbert, G. Renault, M. Rossi, CT-RSA 2019, pp. 272-292
- *Computing isomorphisms and embeddings of finite fields*, L. Brieulle, L. De Feo, J. Doliskani, J.-P. Flori, E. Schost, Mathematics of Computation, vol. 88, pp. 1391-1426
- *Cryptanalysis of NORX v2.0*, C. Chaigneau, T. Fuhr, J. Jean, H. Gilbert, J.-R. Reinhard, Journal of Cryptology, vol. 32(4)
- *GALATICS : Gaussian Sampling for Lattice-Based Constant-Time Implementation of Cryptographic Signatures*, Revisited, G. Barthe, S. Belaid, T. Espitau, P.-A. Fouque, M. Rossi, M. Tibouchi, ACM CCS 2019
- *Harder-Narasimhan theory for linear codes (with an appendix on Riemann-Roch theory)*, H. Randriambololona, Journal of Pure and Applied Algebra 223 (2019) n°7 2997-3030
- *Simple Schnorr Multi-Signatures with Applications to Bitcoin*, G. Maxwell, A. Poelstra, Y. Seurin, P. Wuille, Designs, Codes and Cryptography, vol. 87 (9), 2019
- *Standard lattices of compatibly embedded finite fields*, L. De Feo, H. Randriam, E. Rousseau, Proceedings of ISSAC 2019 (Beijing, July 15-18, 2019) ACM pp. 122-130
- *The quadratic hull of a code and the geometric view on multiplication algorithms*, H. Randriambololona, CoRR abs/1912.06627
- *Two notions of differential equivalence on Sboxes*, C. Boura, A. Canteaut, J. Jean, V. Suder, Designs, Codes and Cryptography, Springer 2019, pp 185-202
- *Multi-Signatures for Blockchains*, Y. Seurin, présentation invitée à la journée Blockchain du LINCS

1.3 Laboratoire exploration et recherche en détection (LED)

- *AutoFeatures : Knowledge-Driven Automatic Feature Engineering for Detection Systems*, P. Collet, A. Beaugnon, C&ESAR 2019
- *Identifying and Characterizing ZMap Scans : a Cryptanalytic Approach*, J. Mazel, R. Strullu, ArXiv
- *IP and TCP Flow Reassembly Testing: From RFC to Pcap*, P. Chifflier, SURICON 2019
- *Memory forensics analysis of IOS XR*, S. Jacob, Hack.lu 2019
- *Scapy-flow: creating test data for parsers/signatures/metadata*, P. Chifflier, SURICON 2019
- *Rust : Towards Better Code Security*, Présentation au GT Sécurité des Systèmes, des Logiciels et des Réseaux du GDR Sécurité informatique

1.4 Laboratoire réseau, protocoles et preuves (LRP)

- *BUS CAN – Se lancer dans l'analyse des communications de votre véhicule*, S. Mainand, MISC hors-série numéro 19, février 2019

1.5 Laboratoire sécurité des composants (LSC)

- *Algorithmic Approaches to Defeat Side Channel Analysis*, E. Prouff, conférence invitée au Boole-an Functions and Applications (BFA) 2019, Florence, Italie

- *Deep Learning to Evaluate Secure RSA Implementations*, M. Carbonne, V. Conin, M.-A. Cornélie, F. Dassance, G. Dufresne, C. Dumas, E. Prouff, A. Venelli, TCHES 2019

- *Evaluating the Security of Implementations Against Side Channel Attacks*, E. Prouff, conférence invitée au Summer School on Real-World Crypto and Privacy, Sibenik, Croatie

- *Fault Injection Characterization on modern CPUs – From the ISA to the Micro-Architecture*, T. Trouchkine, G. Bouffard, J. Clédière, WISTP 2019

- *Gradient Visualization for General Characterisation in Profiling Attacks*, L. Masure, C. Dumas, E. Prouff, COSADE 2019

- *Lower and Upper bounds on the Randomness Complexity of Private Computations of AND*, E. Kushilevitz, R. Ostrovsky, E. Prouff, A. Rosen, A. Thillard, D. Vergnaud, TCC 2019

- *Monomial Evaluation of Polynomial Functions Protected by Threshold Implementations*, S. Landry, Y. Linge, E. Prouff, WISTP 2019

- *Certification and IoT*, G. Bouffard, JAIF 2019, 23 mai 2019 [talk invité]

- *How modern System-on-Chips are vulnerable to fault attacks?*, T. Trouchkine, S. K. Bukasa, M. Escouteloup, R. Lashermes, G. Bouffard, JAIF 2019, 23 mai 2019 [talk invité]

- *Security in modern CPU*, G. Bouffard, Workshop SILM, 21 novembre 2019 [tutoriel]

1.6 Laboratoire de la sécurité des technologies sans-fil (LSF)

- *Agressions Electromagnétiques et Forensics*, J. Lopes-Esteves, CoRi&In 2019, Lille, France

- *A LoRaWAN security Assessment Test Bench*, T. Claverie, J. Lopes-Esteves, Conférence European GNU Radio days 2019, Besançon, France

- *Analysis of Soft Faults induced by IEMI for Elementary Functions and Complex Electronics*, J. Lopes-Esteves, E. Cottais, C. Kasmi, Conférence URSI AP-RASC 2019, New Dehli, Inde

- *Covert Information Embedding in Remote Targets with HPEM*, J. Lopes-Esteves, E. Cottais, ASIAEM 2019, Xian, Chine

- *Electromagnetic Watermarking: exploiting IEMI effects for forensic tracking of UAVs*, J. Lopes-Esteves EMC Europe 2019, Barcelone, Espagne

- *Reducing Complexity of EMC Testing: Improvements for Radiated Experiments using Stochastic Collocation and Bootstrap*, J. Lopes-Esteves, C. Kasmi, S. Lalléchère, S. Girard, P. Bonnet, F. Paladian, L.-O. Frichte, chapitre de l'ouvrage *Uncertainty Modeling for Engineering Applications*, pp. 119-134, Springer, ISBN 978-3-030-04869-3

- *Second Order Soft Tempest: from Cascaded Electromagnetic Interactions to Long Haul Covert Channels*, J. Lopes-Esteves, E. Cottais, C. Kasmi, Conférence URSI AP-RASC 2019, New Dehli, Inde

- *Watermarking Electromagnétique de Drones*, J. Lopes-Esteves, Conférence SSTIC 2019, Rennes, France

- *Estimation statistique de couplages au sein de châssis d'équipements électroniques*, V. Houchouas, E. Cottais, J. Lopes-Esteves, M. Hélier, M. Darces, Y. Chatelon, GT5 GDR Ondes (CNRS), Paris, France

- *Exemples d'interactions entre CEM et SSI*, J. Lopes-Esteves, conférence invitée au GT5 GDR Ondes (CNRS), Paris, France

- *Interactions électromagnétiques et sécurité de l'information*, J. Lopes-Esteves, Conférence plénière du GDR Ondes, Gif-Sur-Yvette, France

1.7 Publications communes entre plusieurs laboratoires

- *Deep Learning for Side-Channel Analysis and Introduction to ASCAD Database*, R. Benadjila, E. Cagli, C. Dumas, E. Prouff, R. Strullu, JCEN 2019 [LED et LSC]

- *Journey to a RTE-free X.509 parser*, A. Ebalard, P. Mouy, R. Benadjila, Conférence SSTIC 2019 [LAM, LRP et LSC]

- *LEIA : The Lab Embedded ISO7816 Analyzer. A Custom Smartcard Reader for the ChipWhisperer*, D. El-Baze, M. Renard, P. Trébuchet, R. Benadjila, Conférence SSTIC 2019 [LSC et LAM]

- *WooKey: Designing a Trusted and Efficient USB Device*, R. Benadjila, A. Michelizza, M. Renard, P. Thierry, P. Trébuchet, ACSAC 2019, San Juan, Puerto Rico [LAM et LSC]

Sous-direction Opérations

- *Designed by geniuses, implemented by morons : an analysis of nation state APT doctrines during geopolitical conflicts*, S. Lefranc et V. Diaz, SAS 2019

- *Active Directory forensics with replication metadata*, CoRIIN 2019, FIRST 2019, BSIDES 2019

- *Analyse du système d'administration à distance des serveurs Dell dénommé iDRAC*, N. Iooss, SSTIC 2019

- *Audit des stratégies de groupe dans les audits Active Directory*, A. Bordes, SSTIC 2019

Rapports sur les menaces et incidents

- *Informations concernant les rançongiciels LockerGoga et Ryuk,* 26 mars 2019

- *Campagne de récupération d'identifiants de connexion : infrastructure malveillante ciblant des institutions gouvernementales et des entités stratégiques,* 2 septembre 2019

- *Supply chain attacks : menaces sur les prestataires de service et les bureaux d'études,* 7 octobre 2019

- *Synthèse sur le rançongiciel BITPAYMER/IENCRYPT*, 21 octobre 2019

- *État de la menace liée aux botnets*, 4 novembre 2019

- *Informations concernant le rançongiciel Clop*, 22 novembre 2019

Autres publications

- *Rapport annuel 2018*

- Magazine interne, deux numéros

: également disponible en anglais

: communications invitées

Noms soulignés : personnes rattachées à l'ANSSI au moment de la publication ou de la soumission de l'article scientifique.

Papiers numériques

➔ Édition 2020

Papiers numériques – Édition 2020
édités par l'Agence nationale
de la sécurité des systèmes
d'information (ANSSI)

Directeur de la publication :
Guillaume Poupard

Cheffe de projet :
Anne-Catherine Belliot

Coordination éditoriale et rédaction :
Aline Barrault,
Anne-Catherine Belliot,
Marang N'Douba

Comité de rédaction :
Yves Auger, Michel Babeau, Charly Berthet,
Louis de Catheu, Valérie Godin,
Geoffroy Hermann et Séverine Oger

Coordination graphique :
Marc Renaudin

Direction artistique,
création graphique et illustrations :
Cercle Studio
www.cerclestudio.com

Crédits :
Pages 4, 11, 13, 14, 29, 37, 49, 53 : ANSSI/Cécilia Conan
Page 13 : Sonic The Hedgehog
Pages 16, 21, 35, 55 : ANSSI/Patrick Gaillardin
Pages 22, 27, 41, 51, 55 : ANSSI
Page 23 : Jacqueline de Haas
Page 15 : ESA/Nadia Imbert-Vier | Jeffrey Galvezo Sales
Page 17 : Droits réservés
Page 31 : Alexandre Gohier
Page 42 : Inria/Photo Pierre Morel
Page 52 : OCDE

Impression :
Imprimerie Baudelaire