17 AVRIL 2018

# DOSSIER DE PRESSE

## L'ANNÉE 2017, UN TOURNANT POUR LA SÉCURITÉ NUMÉRIQUE EN FRANCE

### Un objectif pour 2018 : élever le niveau global de cybersecurité en France

PAR L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

# SOMMAIRE

# L'ANNÉE 2017, UN TOURNANT POUR LA SÉCURITÉ NUMÉRIQUE EN FRANCE

L'année 2017 aura été marquée par de nombreuses attaques informatiques, inédites par leur ampleur et leur sophistication. Pour y faire face, l'ANSSI s'est mobilisée de manière opérationnelle et stratégique pour aider les acteurs nationaux touchés ou menacés.

**2435 signalements d'évènements de sécurité numérique, dont 1621 traités**

Signalement d'évènement de sécurité numérique: description détaillée des caractéristiques techniques d'évènements pouvant laisser penser qu'un incident de sécurité est survenu sur un système numérique.

**794 incidents de sécurité (hors OIV)**

Incident de sécurité : évènement indésirable ou inattendu qui présente une forte probabilité de menacer les systèmes numériques et de compromettre les opérations liées à l'activité d'une organisation.

**20 incidents majeurs de sécurité**

Incident majeur de sécurité : évènement, indésirable ou inattendu, qui menace directement les systèmes numériques et compromet les opérations liées à l'activité d'une organisation.

**12 opérations de cyberdéfense**

Opération de cyberdéfense menée par l'ANSSI : réponse à un incident de sécurité majeur menaçant directement les systèmes numériques et compromettant les opérations liées à l'activité d'une organisation d'importance vitale ou fortement sensible.

**3 crises publiques**

La menace sur les élections présidentielles françaises du 5 mai 2017, le rançongiciel Wannacry du 12 mai 2017 et l'attaque à des fins de sabotage NotPetya du 27 juin 2017.

## LES GRANDES TENDANCES DE LA CYBERMENACE EN 2017

En 2017, l'ANSSI a constaté une évolution de la menace et l'apparition de nouvelles tendances. 2017 a vu apparaître de nouveaux modes opératoires et les attaques ont parfois eu une résonnance dans les sphères politiques, économiques et stratégiques, à l'échelle nationale et internationale.

Retrouvez le cyber panorama 2017 de la menace dans le rapport d'activité 2017 de l'ANSSI

### De nouvelles finalités : la déstabilisation des processus démocratiques et de l'ordre économique

L'ANSSI a constaté deux nouvelles finalités des cyberattaques en 2017.

La première est la **déstabilisation des processus démocratiques.** L'objectif de cette menace est de perturber ou d'influencer le processus démocratique. Suite à la campagne de déstabilisation des élections américaines, la France a activé un plan d'action préventif pour l'élection présidentielle de mai 2017 et les élections législatives de juin 2017.

Une seconde finalité s'est imposée en 2017 : la **déstabilisation de l'ordre économique**. Ciblant des entreprises précises, les attaquants cherchent à perturber l'organisation de leur système économique et leur fonctionnement.

### De nouveaux modes opératoires

L'ANSSI a constaté **une prolifération d'outils d'attaques sophistiqués** en 2017. Ces outils, copiés à l'infini, se sont diffusés très rapidement sur Internet et ont parfois été récupérés par des groupes malintentionnés. Cette multiplicité d'outils et d'acteurs rend plus difficile voire impossible l'identification de l'origine de l'attaque.

En 2017, la France a fait face à une **recrudescence d'attaques aux effets destructeurs,** réalisées à des fins lucratives ou de sabotage. Parmi elles, l'agence observe depuis 2014 une hausse constante des attaques par rançongiciel. NotPetya, l'attaque à des fins de sabotage de juin 2017, en est une parfaite illustration.

À l'échelle mondiale, l'ANSSI a constaté une **multiplication des opérations d'espionnage par compromission d'éditeurs ou de prestataires informatiques.** Ces opérations, menées par des groupes organisés, consistent à capter des informations confidentielles sur un savoir-faire, des individus, des concurrents, un secteur d'activité donné ou encore des organisations, à leur insu.

Enfin, le c**aractère non-discriminant de certaines attaques** s'est imposé en 2017. L'agence a observé une prolifération d'attaques non-ciblées, massives et diffuses, dont l'objectif est de toucher le maximum de personnes, de manière opportuniste. WannaCry en est l'exemple même, le rançongiciel s'étant propagé dans plus de 150 pays, touchant près de 250 000 entités.

## UNE RÉPONSE GLOBALE DE L'ANSSI FACE AUX CYBERATTAQUES DE 2017

Pour répondre aux nombreux incidents survenus en 2017, l'ANSSI a déployé ses **forces opérationnelles** en matière de cyberdéfense. L'agence est intervenue pour stopper des attaques contre des systèmes de l'Etat et des opérateurs d'importance vitale (OIV) et a accompagné la reconstruction des systèmes d'information ciblés.

Néanmoins, répondre n'est qu'une partie de l'action de l'ANSSI. Le rôle de l'agence est également **d'anticiper, veiller, sensibiliser, former et développer un écosystème vertueux à même de prévenir et détecter les attaques.** Justement, 2017 a permis de mettre en lumière tout le faisceau d'actions que l'agence mène au quotidien au-delà de celui, parfois plus visible, de « pompier informatique ».

L'ANSSI assure également une mission de prévention de la menace. L'objectif est de prévenir le succès des attaques informatiques en protégeant les systèmes de l'Etat et des OIV, en anticipant les modes d'attaques et en définissant les mesures de protection. **Le Visa de sécurité** ***via*** la qualification et la certification de solutions numériques participent aussi à la mission de prévention de l'ANSSI.

Pour en savoir plus sur le Visa de sécurité, vous pouvez consulter le dossier de presse « Visa de sécurité ANSSI », accessible sur le site de l'ANSSI : https://www.ssi.gouv.fr/presse/communiques-de-presse/

Enfin, l'agence assure une mission d'information et de sensibilisation. Elle diffuse des recommandations adaptées à ses différents publics, via ses guides, le MOOC SecNum***académie*** et la déploiement de délégués à la sécurité numérique en régions.

Pour Guillaume Poupard, « L'ANSSI développe et entretient une culture de l'innovation en se plaçant non pas comme suiveur mais comme prescripteur. Prescripteur de bonnes pratiques, de bons réflexes, de bonne information. Pour les partager, nos partenaires et nous créons des outils, menons des actions de sensibilisation et soutenons le développement de solutions à la pointe de la technologie pour que chacun puisse s'en emparer et, ainsi, contribuer à cet effort de sécurité numérique qui ne peut être que collectif. »

## UNE RÉELLE PRISE DE CONSCIENCE

Pour Guillaume Poupard, « Des attaques comme WannaCry sont la concrétisation de craintes que nous avions et de scenarios que nous avions imaginés. En 2017, nous avons découvert une nouvelle victime de cyberattaques : la démocratie ! Désormais, à l'aune de ce qu'il s'est passé lors des élections présidentielles, aux Etats-Unis et en France, nos démocraties, et pas uniquement nos économies, nos sociétés, nos administrations, doivent poursuivre leur développement numérique en prenant en compte un risque numérique encore insuffisamment considéré. »

Pour plus d'informations sur le risque démocratique en 2017, vous pouvez consulter le rapport d'activité 2017 de l'ANSSI

2017 aura incontestablement représenté une étape cruciale dans la perception du risque cyber en France. Une année importante de par l'ampleur et l'importante évolution des attaques. Cette année aura enfin permis de déclencher une réelle prise de conscience de la cybermenace chez tout un chacun. Le risque cyber est l'affaire de tous.

Une prise de conscience, également, de la nécessité de développer des outils et des méthodes agiles à même de s'adapter en permanence au caractère désormais mouvant de ces attaques.

## DE NOUVELLES RESPONSABILITÉS POUR TOUS

2017 a installé l'ANSSI comme dépositaire de compétences rares, précieuses et indispensables au respect de notre démocratie, au-delà des compétences décrites par le décret fondateur du 7 juillet 2009. Si les obligations qui résultent de ces attentes sont grandes, l'ANSSI a réussi à allier l'expertise technique et la faculté d'anticipation, tout en s'adaptant en permanence aux besoins de l'État.

L'agence s'appuie sur une approche transverse pour anticiper, prévenir et réagir aux cyberattaques avec pour socle une coordination interministérielle. L'agence a pour objectif de bâtir une véritable relation de confiance avec ses différents publics.

Pour en savoir plus sur la coopération interministérielle, vous pouvez consulter le rapport d'activité 2017 de l'ANSSI

# LES GRANDS ENJEUX POUR 2018

Les grands enjeux qui vont rythmer 2018 sont d'abord européens. Ils comprennent la construction de l'autonomie stratégique européenne pour la sécurité du numérique et la transposition de la directive Network and Information Security (NIS) au niveau national. Les enjeux de 2018 sont ensuite nationaux, avec le renforcement des capacités de détection des attaques, pour élever le niveau de cybersécurité en France.

## LES TRAVAUX EUROPÉENS

L'effort de sécurité numérique ne se conjugue pas qu'au niveau national. Le travail de l'ANSSI s'inscrit également dans une logique européenne et internationale, pas à pas. L'ANSSI a engagé un patient travail de coopération avec la Commission européenne et les États membres de l'Union européenne afin de constituer un ensemble cohérent face à la menace.

Pour en savoir plus sur les travaux européens, vous pouvez consulter le dossier de presse « Sécurité du numérique & Europe : 2018, une année déterminante à l'échelle européenne », accessible sur le site de l'ANSSI : https://www.ssi.gouv.fr/presse/communiques-de-presse/

### Construire l'autonomie stratégique de l'Union européenne

L'autonomie stratégique de l'Union européenne a été identifiée par les autorités françaises parmi les cinq priorités de la Stratégie nationale pour la sécurité du numérique de 2015. **Pour l'ANSSI, la sécurité du numérique de l'Union européenne repose sur sa capacité à garantir son autonomie stratégique en la matière, autour de trois piliers : capacitaire, réglementaire et technologique.**

Pour une Europe forte et de confiance, il est nécessaire de renforcer les capacités nationales des Etats-membres en matière de cybersécurité et de développer une coopération efficace. Les Etats-membres doivent partager des objectifs communs et mobiliser les moyens nécessaires à leur réalisation.

L'ANSSI accueille très favorablement le développement du réseau des CSIRT, une base précieuse d'échanges entre les Etats qui permettra à terme une réponse collective et coordonnée en cas de cyberattaques. L'agence prendra activement part aux négociations sur la révision du mandat de l'ENISA, introduit dans le « Cyber Act » de la Commission européenne.

Selon l'approche française, le marché seul ne peut pas tout faire. L'ANSSI défend l'idée que l'Union européenne doit préserver sa capacité à protéger les citoyens, les entreprises et les Etats membres en matière de sécurité du numérique. Cette protection peut prendre une forme réglementaire, adaptée aux exigences du marché et aux valeurs communes des pays européens. C'est dans ce cadre que les 28 Etats membres doivent transposer dans leur droit national la directive NIS.

L'ANSSI, avec l'appui des acteurs publics et privés, défend la mise en œuvre d'une politique industrielle européenne ambitieuse ainsi que le développement d'une R&D de pointe. Ces deux axes sont indispensables au déploiement de technologies et de services numériques de confiance. De plus, l'agence promeut l'adoption d'un cadre européen de certification de sécurité robuste, qui tirera pleinement bénéfice du retour d'expérience des Etats précurseurs.

## La transposition de la directive Network and Information Security (NIS)

La directive NIS vise à l'émergence d'une Europe forte et de confiance, qui s'appuie sur les capacités nationales des Etats membres en matière de cybersécurité, la mise en place d'une coopération efficace et la protection des activités économiques et sociétales critiques de la nation afin de faire face collectivement aux risques de cyberattaques.

En tant que cheffe de file nationale, l'ANSSI pilote depuis plus d'un an les travaux de transposition, en concertation avec les ministères, les différentes parties-prenantes nationales et ses partenaires européens afin de répondre aux enjeux défendus par ce premier texte européen en matière de cybersécurité.

La loi de transposition de la **directive NIS n° 2018-133 du 26 février 2018** portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité a été publiée au journal officiel le 27 février 2018. La prochaine étape est la publication du décret précisant les mises en œuvre technique et organisationnelle, notamment avec les ministères et fixanrt la liste des services essentiels. Le projet de décret est actuellement au Conseil d'Etat

Pour des éléments complémentaires sur l'autonomie stratégique de l'Union européenne et la directive NIS, consultez le rapport d'activité 2017 de l'ANSSI

# LE DÉVELOPPEMENT DE L'ACTIVITÉ DE DÉTECTION DE L'ANSSI

## Partager la connaissance pour renforcer la capacité de détection des attaques

Pour faire face aux attaques informatiques, l'ANSSI agit sur plusieurs leviers, au premier rang desquels figure la détection des attaques.

La détection d'attaques se définit comme un service de supervision de la sécurité global et maîtrisé. Pour faire de la détection, les experts de l'ANSSI se basent sur leur expertise de la menace stratégique et sur leur connaissance des techniques d'attaque de masse. Les experts cherchent ainsi à détecter des **marqueurs techniques** propres à certains attaquants, tels que l'adresse IP d'un serveur malveillant ou le nom d'un site Internet piégé. Cette activité, d'une très haute technicité, implique une part importante des ressources humaines et techniques du centre opérationnel de l'ANSSI. Bien que la détection n'empêche pas les attaques de se produire, elle participe à la **prévention** de ces dernières et est nécessaire aux opérations de réponse aux incidents.

Le modèle français de cyberdéfense s'appuie sur **une séparation stricte au sein de l'État, des missions offensives, confiées aux services de renseignement, et des missions défensives, assumées par l'ANSSI.** Cette distinction entre les capacités de défense et d'attaque est au cœur de notre modèle démocratique.

La finalité du dispositif de détection de l'ANSSI est de protéger les systèmes de l'État et d'élever le niveau de cybersécurité en France, en détectant au plus tôt les tentatives d'attaques.

## Renforcer les capacités de détection des attaques pour élever le niveau de cybersécurité en France

En 2017, le centre opérationnel de l'ANSSI s'est réorganisé et a créé une division dédiée au développement de la capacité nationale de détection. Cette réorganisation doit favoriser le développement et le maintien à l'état de l'art des moyens techniques de détection. Elle a permis d'accroître la capacité d'échange avec l'État et les OIV, afin d'améliorer la compréhension des systèmes supervisés.

Au quotidien, l'ANSSI développe l'écosystème autour de la détection et partage ses connaissances avec les différents acteurs de cet écosystème. Dans le cadre du décret d'application de la loi de programmation militaire (LPM) 2015, l'ANSSI qualifie des prestataires et des produits de détection d'incidents de sécurité (PDIS).

Enfin, l'ANSSI souhaite renforcer ses liens avec les opérateurs de télécommunication pour renforcer sa capacité de détection.

Pour Guillaume Poupard, « Une meilleure détection des cyberattaques doit passer par une collaboration étroite avec les opérateurs de télécommunication. [...] L'objectif est de mieux utiliser les réseaux de ces opérateurs, dans le respect des libertés et de la neutralité du Net. Il s'agit de leur confier un rôle dans la prévention de cyberattaques et, en cas d'attaques graves et massives, de les soutenir pour contrer celles-ci ».

Pour des éléments complémentaires sur l'activité de détection de l'ANSSI, retrouvez le rapport d'activité 2017 de l'ANSSI

## Les dispositions introduites par l'article 19 du projet de loi relative à la programmation militaire 2019-2025

L'ANSSI se félicite des travaux menés en collaboration avec les opérateurs de télécommunication dans le cadre de l'élaboration de l'article 19 de la Loi de Programmation Militaire 2019-2025. Ce cadre législatif s'inscrit dans une démarche vertueuse et de confiance, visant à élever significativement le niveau de sécurité global de la France.

Le nouveau dispositif comporte deux volets bien distincts.

Le premier volet du dispositif proposé consiste à autoriser les opérateurs de communications électroniques à mettre en œuvre des systèmes de détection dans leurs réseaux afin de détecter les attaques informatiques visant leurs abonnés. Pour leur permettre de détecter des attaques sophistiquées, l'ANSSI fournira aux opérateurs des marqueurs d'attaque.

Si l'attaque détectée concerne un opérateur d'importance vitale ou une autorité publique, l'ANSSI pourra demander des informations techniques complémentaires pour caractériser l'attaque et établir des mesures de protection et de remédiation adaptées avec la victime.

Le second volet du dispositif donne la possibilité à l'ANSSI, lorsqu'elle a connaissance d'une menace grave et imminente sur les systèmes d'une autorité publique ou d'un OIV, de mettre en place un dispositif de détection local et temporaire sur un serveur d'un hébergeur ou un équipement d'un opérateur de communications électroniques contrôlé par un attaquant. Le dispositif de détection est mis en oeuvre pour la durée et dans la mesure strictement nécessaires à la caractérisation de la menace.

## Le rôle de contrôle de l'ARCEP, gage de confiance

Le respect du cadre juridique, dans lequel s'incriront les nouvelles missions de l'ANSSI, sera contrôlé par une autorité administrative indépendante. Compte-tenu de ses compétences dans le domaine des communications électroniques, l'Autorité de régulation des communications électroniques et des postes (ARCEP) est apparue comme la plus à même de s'en charger.

L'ANSSI se réjouit du dialogue qu'elle sera amenée à avoir avec l'ARCEP, sur la base de leur compétence partagée.

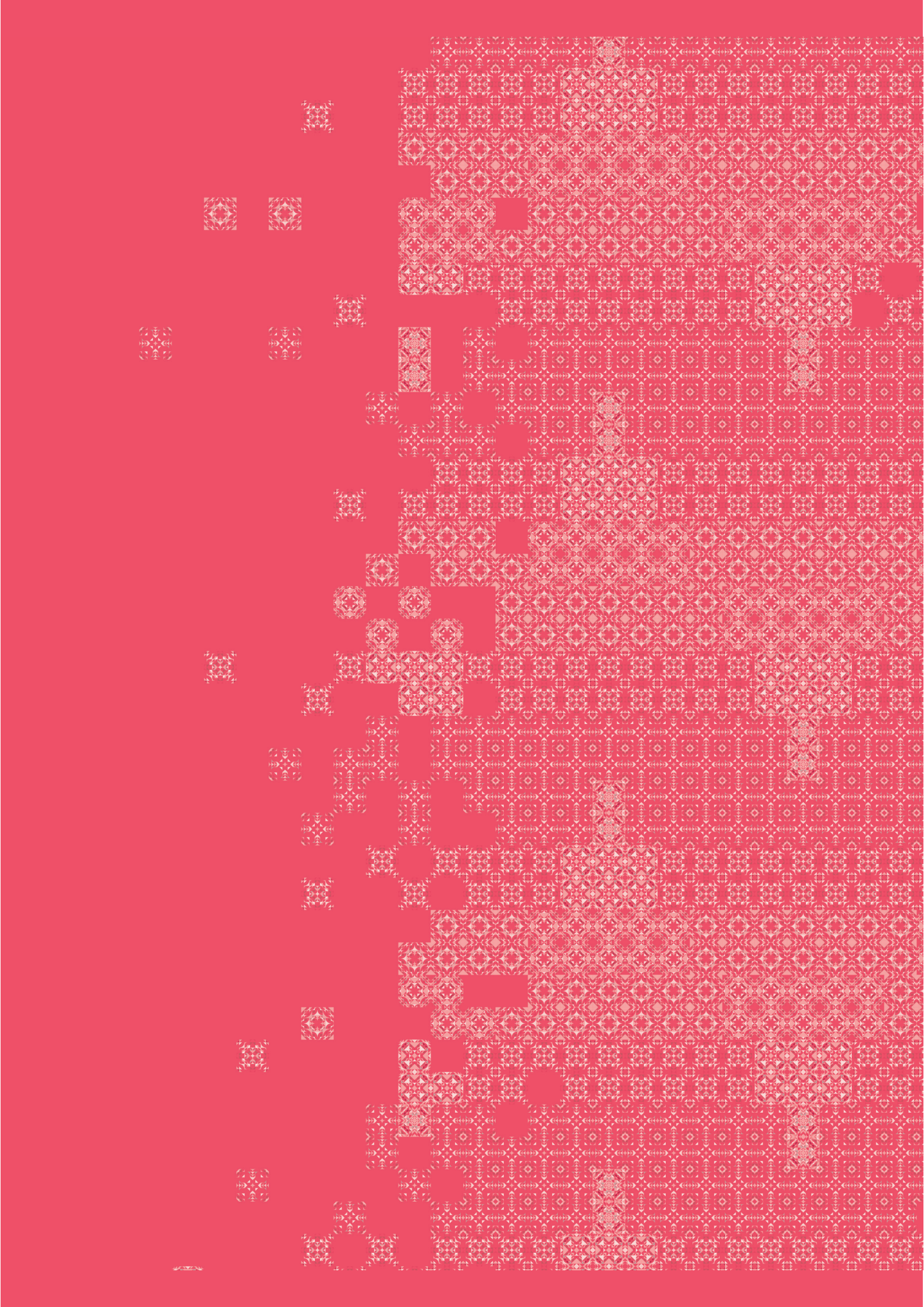
L'année 2017 s'est révélée comme un véritable tournant pour le cyber en France. L'année s'est caractérisée par une hausse constante des effectifs de l'ANSSI avec 140 agents engagés, pour un accroissement des effectifs de 50 personnes. Ces recrutements ont majoritairement concerné le cœur de métier d'expertise en sécurité des systèmes d'information. Aujourd'hui, la France doit poursuivre sa montée en puissance afin de faire face à une menace constante et en perpétuelle évolution. Il s'agit pour 2018, de se donner collectivement les moyens et les ressources pour répondre efficacement et rapidement à une menace en forte progression.


## À PROPOS DE L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n° 2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale.
L'agence assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP

www.ssi.gouv.fr — communication@ssi.gouv.fr




**CONTACTS PRESSE :**

**Margaux Vincent**
margaux.vincent@ssi.gouv.fr
01 71 75 84 04

**Anne-Charlotte Brou**
anne-charlotte.brou@ssi.gouv.fr
01 71 75 82 97