RÉPUBLIQUE
FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

# RAPPORT D'ACTIVITÉ 2025

# Sommaire

# Édito de Vincent Strubel

1 263. C'est le nombre d'organisations qui ont participé à l'exercice de crise cyber REMPAR25. Le nombre est inédit, mais demeure modeste à l'échelle de la Nation. La France doit pourtant se préparer à un scénario d'attaques informatiques beaucoup plus massives. C'est le défi que nous avons devant nous et qui est matérialisé dans les textes stratégiques parus cette année. *Le Panorama de la cybermenace* 2025 en témoigne, l'effet de masse est déjà présent et la menace cyber est une réalité du quotidien qui nous impose d'intensifier nos efforts.

Ce scénario n'est pas une fatalité, il se prépare collectivement et ces travaux sont engagés. L'année 2025 a été à ce titre significative en termes d'avancées, portées en première ligne par les agentes et agents de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui conduisent des exploits au quotidien.

Pour la première fois, la France a attribué des attaques informatiques intervenues sur son territoire au renseignement militaire russe. Cette démarche est issue d'un travail technique rigoureux conduit avec l'ensemble des membres du Centre de coordination des crises cyber (C4). Elle envoie un signal fort à nos agresseurs, actuels et potentiels, sur les capacités de la France à entraver leurs attaques.

En matière de résilience, l'Agence a poursuivi ses travaux d'« outillage » dans une logique partenariale avec les acteurs de l'écosystème cyber. La menace à laquelle nous faisons et allons faire face nous invite à faire évoluer nos approches traditionnelles. Dans cette perspective, si le cadre réglementaire est un

levier incontournable pour la matière cyber sur lequel nous nous investissons fortement, aux niveaux national et européen, il n'est pas suffisant. Nous devons aussi penser à de nouveaux modes d'action à l'instar des exercices de crise massifiés ou à des démarches incitatives telles que la certification, qui permettra aux petites et moyennes entreprises de bénéficier d'une présomption de conformité au référentiel de mesures de cybersécurité NIS 2.

Dans le champ technologique, l'année a été marquée par d'importants travaux de doctrine et de recommandations, et l'étoffement conséquent de l'offre de solutions de confiance. Les ruptures technologiques que nous vivons et vivrons, nous obligent là aussi à repenser nos modes d'action. La multiplication des vulnérabilités, le risque de coupure technologique, l'extraterritorialité du droit, la complexification des technologies sont autant de risques à considérer dans nos approches.

Les défis sont grands, mais nous saurons les relever collectivement.

**Vincent Strubel**
Directeur général de l'ANSSI

# Missions de l'ANSSI

Service du Premier ministre créé en 2009 et placé sous l'autorité du secrétaire général de la défense et de la sécurité nationale, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité et de cyberdéfense en France. Le modèle français de la cybersécurité repose sur une séparation claire, au sein de l'État, entre les missions défensives et offensives, et l'ANSSI est chargée de coordonner le champ de la défense et de la protection des systèmes d'information.

La raison d'être de l'Agence est ainsi de construire et d'organiser, en interministériel, la protection de la Nation face aux cyberattaques, et de contribuer à la stabilité du cyberespace. Son action s'inscrit dans le cadre des missions régaliennes de l'État, au service d'un objectif général de politique publique de sécurité et de résilience des administrations, de l'économie et de la société dans son ensemble.

L'action de l'ANSSI se traduit en cinq grandes missions :

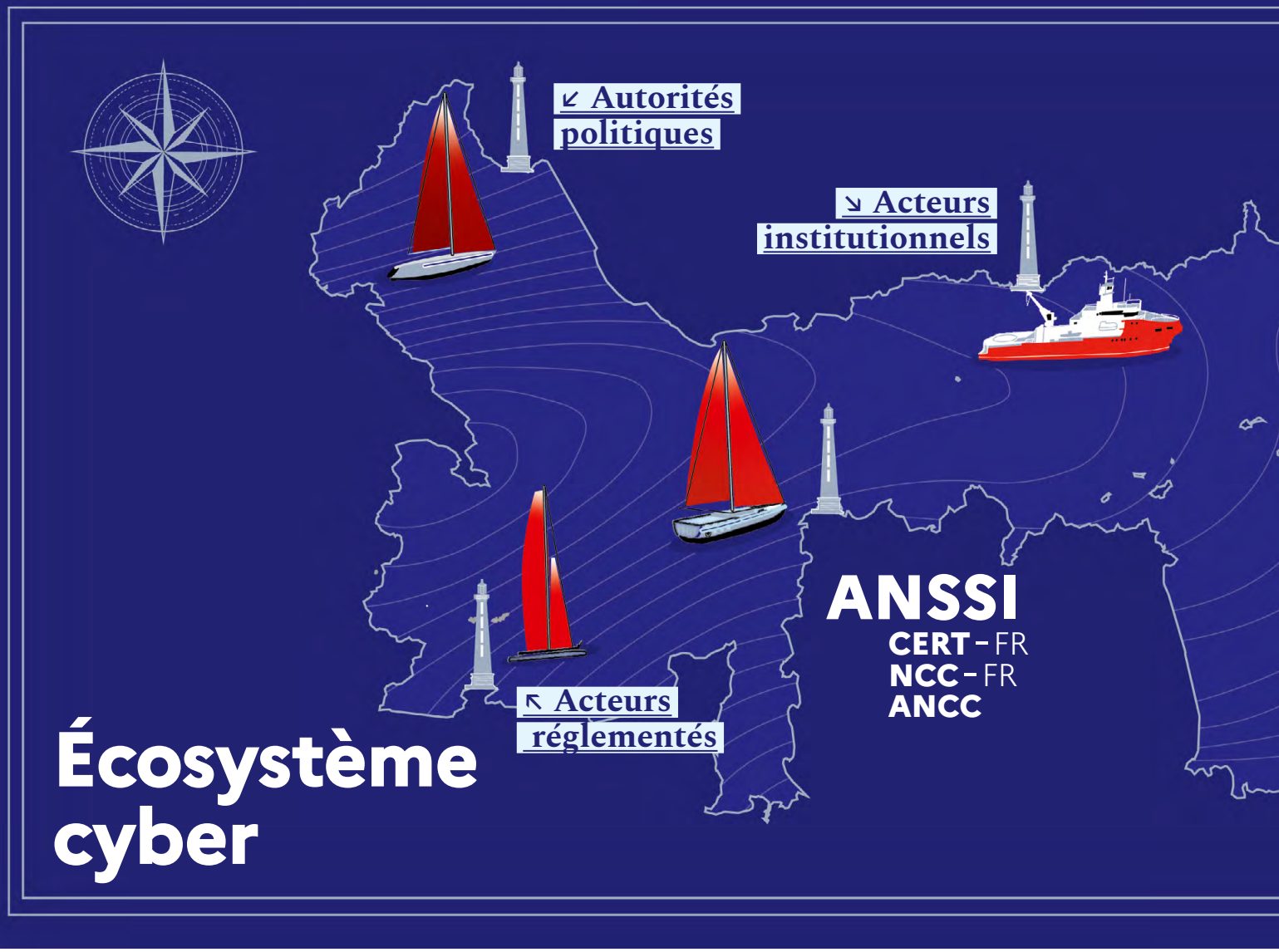
- → **Défendre** les systèmes d'information critiques et les victimes de cyberattaques d'ampleur ;
- → **Connaître** l'état de l'art de la cybersécurité et les menaces du cyberespace ;
- → **Partager** de la connaissance, des recommandations et de l'expertise en sureté numérique ;
- → **Accompagner** l'écosystème national et international ;
- → **Réguler** les organisations, les produits et les services de cybersécurité.

L'Agence est organisée en quatre sous-directions et une mission sous le pilotage et la coordination de la direction générale :

- **La sous-direction Expertise** élabore et diffuse les bonnes pratiques de cybersécurité et contribue à améliorer l'offre de produits et services de cybersécurité, pour accompagner la sécurisation des organisations.
- **La sous-direction Opérations** assure la mise en œuvre de la fonction d'autorité de défense des systèmes numériques d'intérêt pour la Nation dévolue à l'ANSSI et constitue le centre de réponse à incident national et gouvernemental pour la France (CERT-FR).
- **La sous-direction Ressources** est responsable de la programmation et de l'exécution des activités de gestion et de pilotage des ressources financières, humaines, mobilières et immobilières, et de l'expertise et de l'accompagnement légal de l'ANSSI.
- **La sous-direction Stratégie** développe et pilote la contribution de l'ANSSI à l'élaboration et à la mise en œuvre des politiques publiques en faveur de la sécurité du numérique, tant au niveau territorial national qu'européen et international.
- **La mission Contrôles et Supervision** conçoit et met en œuvre la politique de supervision et de contrôle de l'ANSSI au titre de certaines réglementations européennes (directive NIS, règlements CSA et eIDAS) et nationales (SAIV, certification).

### ↘ Une Agence sur quatre sites

L'ANSSI est implantée sur quatre sites : l'Hôtel national des Invalides et la tour Mercure à Paris, le Campus Cyber à La Défense et ArteFact à Rennes. L'Agence est ainsi plus proche de ses bénéficiaires et peut plus facilement nouer des partenariats avec ses partenaires et renforcer les synergies entre acteurs publics et privés. ●




# Écosystème cyber

## ↘ Autorités politiques

**Élus locaux**
**Gouvernement**
**Parlement**
**Premier ministre**
**Président de la République**

## ↘ Acteurs institutionnels

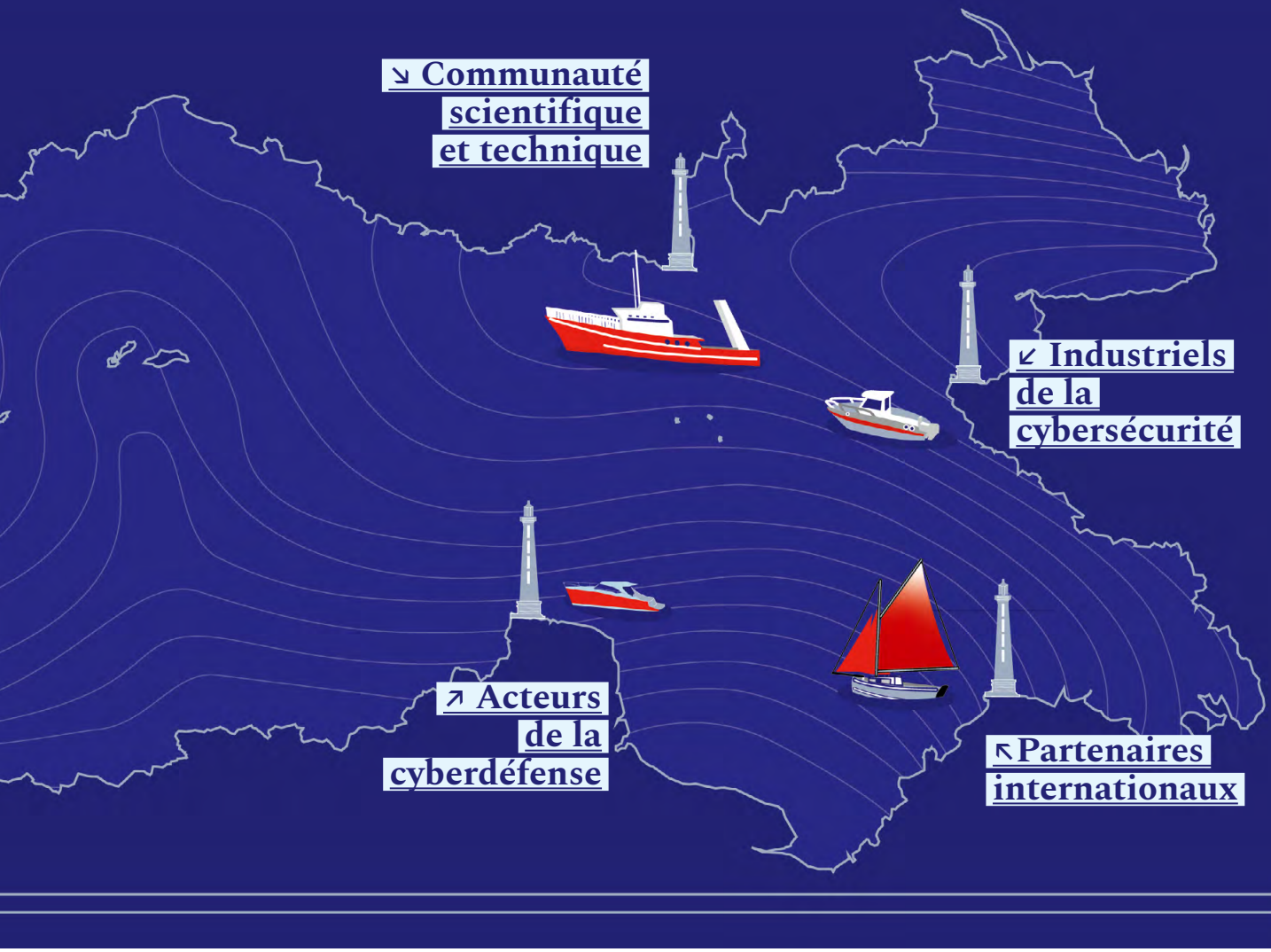
**Acteurs publics et privés de l'investissement** (Bpifrance, SGPI, etc.)
**Autorités de contrôle** (ARCEP, autorité de la concurrence, CNIL, etc.)
**Autorités sectorielles** (ACPR, AMF, etc.)
**Collectivités territoriales**
**Fédérations professionnelles**
**Ministères** (DGA, DGE, DINUM, DITP, etc.)
**SGDSN** : Secrétariat général de la défense et de la sécurité nationale
**Organismes de normalisation** (AFNOR, ETSI, etc.)
**Parquet de Paris** (section J3)

## ↘ Acteurs réglementés

**Administrations**
**OCE** : Opérateurs de communication électronique
**OIV** : Opérateurs d'importance vitale
**OSE** : Opérateurs de services essentiels
**EE :** entités essentielles
**EI :** entités importantes

## ↘ Acteurs de la cyberdéfense

**C4** : Centre de coordination des crises cyber (ANSSI, COMCYBER, DGA, DGSE, DGSI, MEAE)
**CSIRT privés** : Centres de réponse aux incidents cyber privés
**CRC** : Centres de ressources cyber
**CSIRT ministériels** : Centres de réponse aux incidents cyber ministériels
**CSIRT sectoriels** : Centres de réponse aux incidents cyber sectoriels
**CSIRT territoriaux** : Centres de réponse aux incidents cyber territoriaux
**Gendarmerie nationale**
**GIP ACYMA** : Groupement d'intérêt public Action contre la cybermalveillance
**InterCERT France** : Première communauté de CERT en France
**Police nationale**




*Cette liste est non-exhaustive*

### ↘ Communauté scientifique et technique

**Acteurs de la recherche** (CEA, CEA-Leti, CNRS, INRIA, etc.)
**Conseil scientifique de l'ANSSI**
**Entités labellisées SecNumedu et SecNumedu-FC**: Labels de formations de l'enseignement supérieur et de formations continues spécialisées en cybersécurité
**Grandes écoles**
**Organismes de formation**
**Universités**

### ↘ Partenaires internationaux

**CERT-EU**: Centre de réponse aux incidents cyber pour les institutions européennes
**CSIRTs Network**: Réseau des centres de réponse aux incidents cyber de l'Union européenne
**ECCC**: Centre de compétences cyber européen
**ENISA**: Agence de l'Union européenne pour la cybersécurité
**EU-CyCLONe**: Réseau européen des organisations de liaison en cas de crise cybernétique
**Homologues européens et internationaux**
**NCC**: Centres de coordination nationaux
**OCDE**: Organisation de coopération et de développement économiques
**OTAN**: Organisation du traité de l'Atlantique nord

### ↘ Industriels de la cybersécurité

**Campus Cyber national et régionaux**
**CESTI**: Centres d'évaluation de la sécurité des technologies de l'information
**Incubateurs**
**Offreurs de confiance** (PACS, PAMS, PASSI, PDIS, PRIS, PVID, prestataires SecNumCloud, prestataires de services de confiance eIDAS, prestataires EBIOS *Risk Manager*, offreurs CC, offreurs CSPN, offreurs MIE)
**Offreurs de solutions de cybersécurité**

# 2025 en chiffres

**658** agents [1]

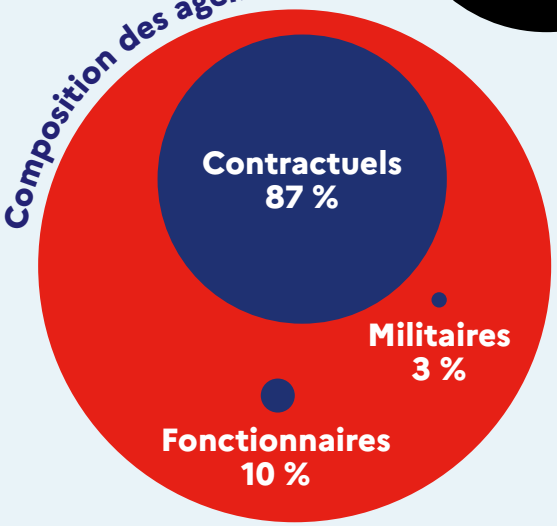
**38** ans de moyenne d'âge

**499** visas de sécurité délivrés

**369** qualifications

**130** certifications

Composition des agents




**44,2** millions d'euros de budget (hors masse salariale) [2]

**147 027** attestations SecNum*académie* délivrées

**17** formations labellisées SecNumedu-FC

**26** formations labellisées SecNumedu

**1 543** personnes formées au CFSSI

**1 366**
incidents [3]
+ 0,4 % par rapport à l'année 2024

**84 762**
rapports d'audits automatisés (ADS et SILENE)
+ 43 % par rapport à l'année 2024

**3 586**
événements de sécurité [4]
- 22 % par rapport à l'année 2024

**13**
rapports menaces et incidents publiés sur le site du CERT-FR

**65**
évaluations TEMPEST d'équipements réalisées

**51**
audits TEMPEST sur site réalisés

**265**
avis TEMPEST délivrés

**43**
structures de normalisation dont 11 françaises ayant bénéficié d'une participation ANSSI
+ 30 % par rapport à l'année 2024

**1**
autorisation délivrée en tant qu'organisme d'évaluation de la conformité au titre de EUCC

**22**
articles scientifiques publiés

**1**
avis technique publié

**1**
étude de marché

**16**
logiciels publiés en *open source*

**28**
guides techniques publiés

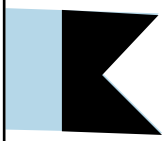
[1] Personnels civils et militaires hors stagiaires et apprentis.
[2] Dont 16,3 millions d'euros apportés par un amendement gouvernemental en septembre 2025 au profit du déploiement de la Stratégie nationale de cybersécurité 2026-2030.
[3] Événements de sécurité pour lesquels l'ANSSI confirme qu'un acteur malveillant a conduit des actions avec succès sur le système d'information de la victime.
[4] Événements portés à la connaissance de l'ANSSI et qui ont donné lieu à un traitement par les équipes opérationnelles.

# Temps forts 2025

## JANVIER

**9 janvier 2025**
Clôture de l'appel à projets national « Soutien aux PME et startups pour renforcer leurs compétences dans le domaine de la cybersécurité » lancé par le Secrétariat général pour l'investissement en charge de France 2030, l'ANSSI et Bpifrance. 18 entités lauréates

## FÉVRIER



**10-11 février 2025**
Publication d'une analyse de risques sur l'IA et organisation d'un exercice de crise dans le cadre du Sommet pour l'action sur l'IA, et annonce par le Gouvernement de la création de l'Institut national pour l'évaluation et la sécurité de l'IA (INESIA)

**20 février 2025**
Publication de l'état de la menace sur le secteur du *cloud computing*

## MARS

**4 mars 2025**
3e journée du CERT-FR rassemblant 230 représentants de CSIRT

**6 mars 2025**
Publication du Plan stratégique de l'ANSSI 2025-2027

**11 mars 2025**
Publication du Panorama de la cybermenace 2024

**12 mars 2025**
Adoption par le Sénat en première lecture du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

**14 mars 2025**
MonServiceSécurisé est désigné service à impact national par la direction interministérielle du numérique

**28 mars 2025**
Publication du programme de travail *Digital Europe* (financements européens pour l'écosystème cyber) publié par la Commission européenne

**31 mars 2025**
Deux premiers certificats européens EUCC délivrés par l'ANSSI, à la suite de l'autorisation, pour le niveau élevé, du centre de certification national (CCN)

## AVRIL

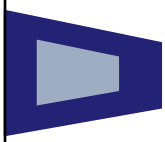
**2 avril 2025**
Lancement du portail de services MesServicesCyber

**2 avril 2025**
Publication du premier rapport d'activité conjoint par les CSIRT territoriaux

**18-27 avril 2025**
Compétition France Cybersecurity Challenge (FCSC) 2025 organisée par l'ANSSI

**29 avril 2025**
Attribution publique par la France d'un ensemble de cyberattaques au renseignement militaire russe (GRU)

## MAI



**15 mai 2025**
Consultation d'experts sur les signalements liés aux vulnérabilités et la protection des activités des hackers éthiques

## JUIN

**10 juin 2025**
Publication de la 4e édition de l'Observatoire des métiers sur les professionnels de la cybersécurité et le marché du travail en cybersécurité en France

## JUILLET

**14 juillet 2025**
Publication de la Revue nationale stratégique 2025

## AOÛT

**22 août 2025**
Lancement d'un appel à manifestation d'intérêt (AMI) pour le renforcement de l'accompagnement local aux enjeux de cybersécurité

## SEPTEMBRE

**3 septembre 2025**
Publication du document « *A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity* », co-signé par 18 agences gouvernementales américaines, asiatiques et européennes dont l'ANSSI

**10 septembre 2025**
Adoption du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, en commission spéciale de l'Assemblée nationale

**18 septembre 2025**
Exercice de crise d'origine cyber massifié REMPAR25

## OCTOBRE

**16 octobre 2025 :**
Attribution de deux premiers Visas de sécurité ANSSI pour des certifications de solutions intégrant de la cryptographie post-quantique

**28 octobre 2025**
Mise à jour du référentiel Prestataires de réponse aux incidents de sécurité (PRIS) avec intégration de l'activité « gestion de crise d'origine cyber »

## NOVEMBRE

**4 novembre 2025**
Journée du conseil scientifique de l'ANSSI

**19 novembre 2025**
Déclaration conjointe BSI (*Bundesamt für Sicherheit in der Informationstechnik*) – ANSSI sur les critères de souveraineté numérique du *cloud* : « *Joint Statement by ANSSI and BSI on Cloud Sovereignty Criteria* »

**24 novembre 2025**
Lancement du préenregistrement NIS 2

**25 novembre 2025**
Transfert officiel de la présidence du groupe de travail « cyber » du G7 de l'agence homologue canadienne, le CCCS (*Canadian Centre for Cyber Security*), vers l'ANSSI

**26 novembre 2025**
Publication de l'état de la menace sur les équipements mobiles depuis 2015

## DÉCEMBRE

**8 décembre 2025**
Notification d'un marché au CEA Leti, pour une étude de faisabilité d'un composant de sécurité sur une architecture RISC-V répondant aux contraintes d'utilisation dans des produits de sécurité utilisés en mobilité

**27 décembre 2025**
Journée de l'innovation de l'ANSSI, rendez-vous annuel auquel ont été conviés des utilisateurs et utilisatrices, partenaires et agents de l'ANSSI afin de présenter la feuille de route de l'ANSSI en matière d'innovation et d'échanger autour des besoins et idées de ses bénéficiaires

# De nouvelles orientations stratégiques

**L'année 2025 a été marquée par la publication de nouvelles orientations stratégiques nationales en matière de défense et de sécurité nationale. L'action de l'ANSSI s'inscrit dans ce cadre refondu.**

## La Revue nationale stratégique 2025 : se préparer à un scénario d'escalade de tensions

Parue en 2025, la *Revue nationale stratégique* vise à préparer la France à un environnement dégradé dans lequel le cyberespace est devenu un espace de compétition, de contestation et parfois même d'affrontement désinhibé, en miroir des tensions géopolitiques et des rivalités internationales.

Dans le domaine de la cybersécurité, est fixé pour la France l'objectif stratégique d'avoir « une résilience cyber de premier rang ». Cette résilience doit s'entendre comme la capacité pour la France à surmonter une vague importante d'attaques informatiques qui pourrait remettre en cause le fonctionnement de la Nation. Cet objectif stratégique s'entend également comme le maintien de la France dans le premier cercle des pays en termes de maturité cyber.

La *Revue nationale stratégique* repose sur un scénario central : celui d'une guerre aux portes de l'Europe qui engage les forces armées françaises, et se traduit par une démultiplication des menaces hybrides, manipulations de l'information, attaques informatiques, attentats, sabotages… sur le territoire national. Ce scénario n'est pas une prédiction mais une anticipation, et doit aider l'ensemble de la Nation à se préparer à faire face à un tel contexte au vu de la détérioration des relations internationales. Face au caractère polymorphe des menaces auxquelles la France doit se préparer, l'État, dans sa dimension centralisatrice et verticale, ne pourra pas suffire ; la Revue promeut à ce titre une logique plus horizontale, embarquant tous les pans de la Nation.

## La Stratégie nationale de cybersécurité 2026-2030 : le volet cyber de cette préparation

Parue en janvier 2026, la *Stratégie nationale de cybersécurité* est la déclinaison du volet cyber de la *Revue nationale stratégique*. Structurée en cinq piliers, elle appelle à une mobilisation collective pour former davantage de talents dans le domaine de la cybersécurité, élever le niveau général de cybersécurité, mieux préparer la Nation aux crises d'origine cyber, entraver plus efficacement la cybermenace, et préserver la maîtrise des fondements numériques de l'économie et de la société dans un contexte de dépendances technologiques accrues. Elle pose également le constat que la résilience cyber de la France dépend de celle de ses partenaires et alliés

européens et internationaux, ainsi que de la sécurité et de la stabilité du cyberespace dans son ensemble. Elle affirme à ce titre la position de la France comme une puissance cyber responsable et solidaire, en renforçant ses capacités d'influence et de coopération.

La *Stratégie nationale de cybersécurité* conforte le modèle de cyberdéfense français qui sépare les capacités défensives et offensives. L'ANSSI, en tant qu'autorité nationale de cyberdéfense et de cybersécurité, a pour rôle de coordonner les capacités défensives. La stratégie fait aussi évoluer la gouvernance nationale de cybersécurité pour mieux y intégrer les parties prenantes.

### Le plan stratégique de l'ANSSI 2025-2027 : au coeur d'un collectif pour une nation cyber-résiliente

Le plan stratégique de l'ANSSI pour 2025-2027 s'inscrit en cohérence avec ces documents stratégiques. Il part de plusieurs constats : d'un côté, une cybermenace qui affecte désormais tous les pans de l'économie et de la société avec une diversification des attaques informatiques, une situation internationale toujours plus conflictuelle, une évolution rapide des technologies du numérique, un contexte national et international qui exige de manière croissante la prise en compte des enjeux sociétaux tels que les impacts environnementaux du numérique. De l'autre, pour répondre à ces enjeux, une offre de solutions et de services de cybersécurité qui s'est étoffée, un cadre réglementaire renforcé avec l'extension des missions de contrôle de l'Agence et l'élargissement du périmètre des organisations et produits régulés, ainsi que des agendas politiques national et européen qui placent au cœur de leurs priorités la sécurité de l'Europe.

Dans la lignée de la *Stratégie nationale de cybersécurité*, il invite à faire évoluer l'action publique en cybersécurité, dans sa gouvernance et ses modes d'action. L'ANSSI entend incarner cette évolution, en refondant ses modes d'interaction avec ses parties prenantes et en permettant à un réseau élargi d'acteurs de la cybersécurité d'amplifier leurs actions et leur impact en ce domaine.

Le plan stratégique se décline en quatre grands axes :

- Amplifier et coordonner la réponse cyber face à la massification de la menace : l'action publique a renforcé ces dernières années le cadre réglementaire et accompagné l'essor de nouveaux acteurs de la cybersécurité. Cet axe vise ainsi à renforcer cette dynamique en assurant un soutien et une meilleure articulation de ces dispositifs, ainsi qu'une plus grande lisibilité des services pour les bénéficiaires ;

- Développer les expertises indispensables pour contrer les menaces cyber : cet axe vise à entretenir un haut niveau d'expertise et préserver une maîtrise autonome des savoirs scientifiques et technologiques en matière de cybersécurité, en lien avec les évolutions de la menace et des technologies ;

- Promouvoir une action cyber européenne et internationale efficace : cet axe vise à soutenir une mise en œuvre harmonisée des actions cyber aux niveaux européen et international, en s'engageant en particulier dans la mise en œuvre de la révision du cadre de certification européen et dans les réseaux de coopération européens et internationaux ;

- Renforcer la prise en compte des enjeux sociétaux dans l'action de l'ANSSI : cet axe vise en particulier à consolider la prise en compte de la question environnementale dans les recommandations et les activités de l'Agence et à développer la politique de diversité au sein de l'ANSSI et de la filière de la cybersécurité.

# Face à la massification de la menace, déployer et coordonner la réponse cyber

Face à l'intensification et la diversification de la menace qui pèse sur les systèmes d'information de la Nation, l'ANSSI déploie et coordonne un ensemble de dispositifs de cybersécurité permettant d'augmenter le niveau de préparation et de sécurité des organisations. Ce travail a été poursuivi cette année avec l'écosystème cyber, aux niveaux national, européen et international.

# La réglementation au service de la résilience cyber

## Élever le niveau de cybersécurité des organisations avec la directive NIS 2

En 2025, l'ANSSI a poursuivi le travail de préparation de la mise en œuvre de la directive NIS 2 (*Network and Information Security*, ou sécurité des réseaux et des systèmes d'information), qui invite plusieurs milliers d'entités en France à renforcer leurs moyens de cyberdéfense. Elle concerne les administrations de l'État, les collectivités territoriales et les moyennes et grandes entreprises qui interviennent dans 18 secteurs d'activité, et distingue deux catégories d'entités régulées, les entités essentielles (EE) et les entités importantes (EI).

La directive NIS 2 fait évoluer les missions de l'Agence, en ajoutant à l'accompagnement et la défense de ses bénéficiaires des prérogatives de contrôle et de supervision des entités concernées par la réglementation.

Les travaux de transposition de la directive, engagés depuis 2022, se concrétisent dans les dispositions prévues dans le projet de loi relatif à la résilience des infrastructures

« Pour les entités, NIS 2 est une nécessité autant qu'une opportunité. Au-delà d'une obligation légale, c'est un levier pour moderniser, sécuriser et renforcer la confiance dans les services publics et les entreprises. »

Aurélie Cotton
Cheffe d'État-Major de la
Sous-direction Stratégie de l'ANSSI

critiques et au renforcement de la cybersécurité. En 2025, des jalons importants ont été franchis, avec son adoption en première lecture au Sénat le 12 mars 2025 et en commission spéciale à l'Assemblée nationale le 10 septembre 2025.

L'ANSSI a également animé tout au long de l'année des échanges interministériels et avec les associations et fédérations professionnelles et les associations d'élus locaux sur les projets de texte réglementaires relatifs à cette transposition. En complément du futur cadre NIS 2 qui vise à protéger d'une menace cybercriminelle, l'Agence a également travaillé avec des opérateurs critiques et leurs ministères coordinateurs à la mise à jour du référentiel de cybersécurité des entités portant des missions d'importance vitale pour l'État qui font face à une menace stratégique (d'origine étatique).

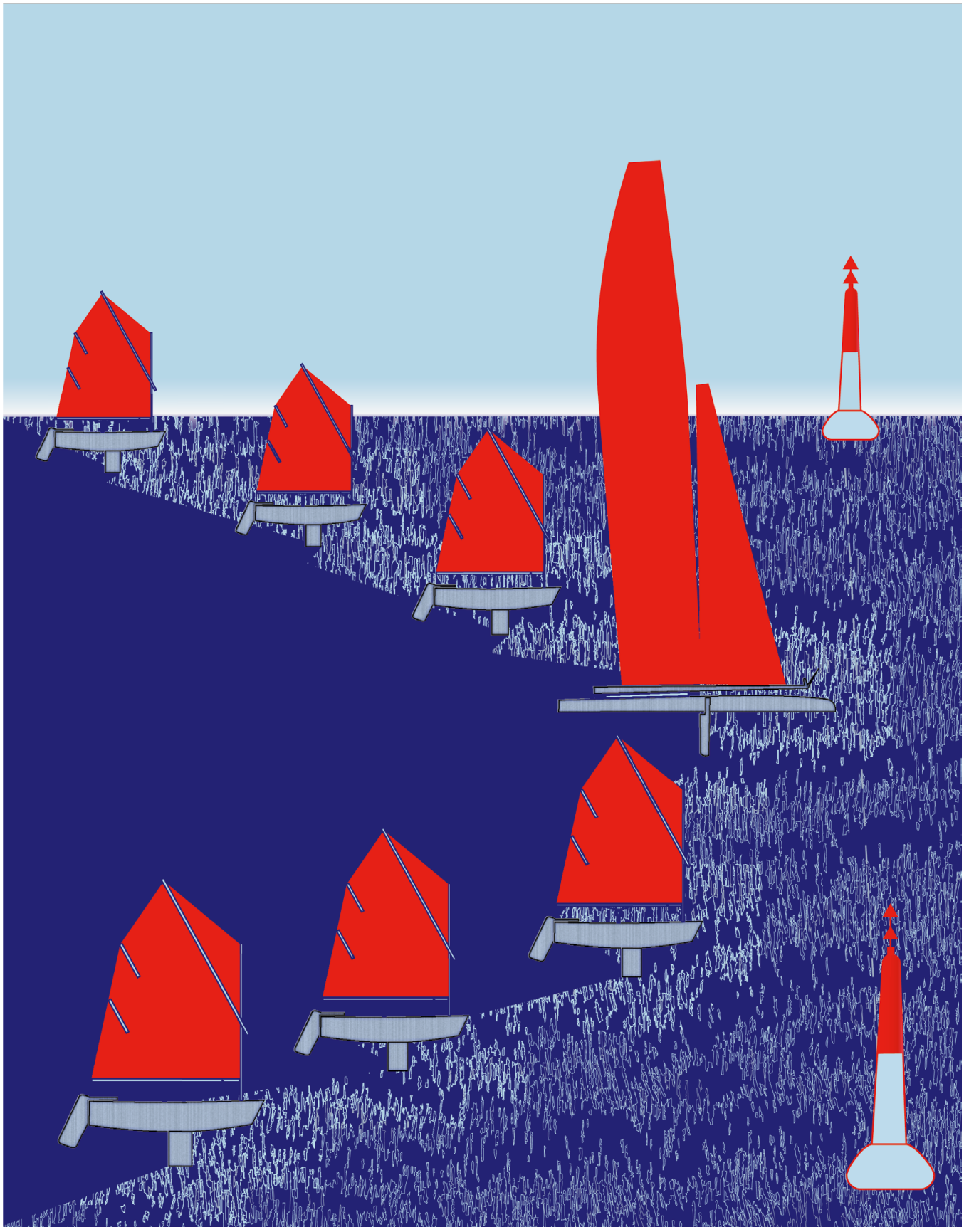
Afin de préparer au mieux la mise en œuvre de ce futur cadre réglementaire, les organisations et les collectivités territoriales peuvent s'engager dans une démarche de sécurisation cohérente. Concrètement, ce mouvement peut s'articuler aujourd'hui autour de plusieurs types de mesures et d'actions concrètes :

- **S'informer :** les délégués territoriaux de l'ANSSI se tiennent à disposition des adhérents pour présenter ce cadre réglementaire. Un ensemble de ressources clés en main est également déjà disponible sur la plateforme MesServicesCyber. Ces ressources seront complétées et renforcées au fil des mois par des fiches pratiques, formulaires types, pour accompagner les collectivités dans leur démarche de sécurisation.

- **Se pré-enregistrer :** en attendant l'entrée en vigueur de l'obligation d'enregistrement qui interviendra avec la publication des textes réglementaires associés au projet de loi, l'ANSSI a mis en ligne, le 24 novembre 2025, un service de pré-enregistrement pour les futures entités assujetties à NIS 2, ouvert à date aux entreprises. L'ambition est double : permettre aux organisations volontaires d'anticiper cette première obligation et d'accéder à certaines ressources spécifiques, d'une part, et disposer d'informations utiles pour adapter au mieux les ressources d'accompagnement, d'autre part. Pour les entreprises qui ont des doutes sur le périmètre d'application, un service est à leur disposition pour tester leur éligibilité à NIS 2. Ce pré-enregistrement permettra aux entités de bénéficier d'un enregistrement facilité lorsque la phase d'enregistrement obligatoire démarrera. Il constitue un premier pas pour les entités vers le respect de leurs obligations.

- **Mettre en œuvre de premières mesures de sécurité :** la version « bêta » du référentiel pour les organisations assujetties à NIS 2 (hors acteurs du numérique) est à présent disponible. Résultat d'un long et fructueux travail de consultation avec l'écosystème en 2024 et 2025, ce référentiel liste les mesures recommandées par l'ANSSI pour atteindre les objectifs de sécurité fixés par NIS 2 et partage des bonnes pratiques de cybersécurité. Le respect de ces objectifs de sécurité, qui recouvrent les grands domaines classiques de la cybersécurité, induisent la mise en œuvre de mesures proportionnées au statut d'entité importante et essentielle. Ce référentiel est une version « bêta » susceptible d'ajustements pour tenir compte des discussions parlementaires et des travaux réglementaires.

- **Notifier ses incidents :** l'Agence permet aux organisations et aux collectivités territoriales de procéder à la notification de leurs incidents cyber sur la plateforme ClubSSI, et de solliciter une assistance 24h/24 par téléphone au 3218. Au-delà de la future obligation de notification, les entreprises et collectivités futures assujetties à NIS 2 peuvent bénéficier de l'assistance du CERT-FR et de son réseau de partenaires.



# Le règlement sur la cyber-résilience, pendant de la directive NIS 2 pour les fournisseurs de solutions numériques

Pendant de NIS 2 pour les fournisseurs de solutions numériques, le règlement européen sur la cyber-résilience (*Cyber Resilience Act*) permet de développer un marché européen de produits numériques de confiance.

Ce règlement européen, publié le 20 novembre 2024, définit des exigences minimales de cybersécurité pour l'ensemble des produits comportant des éléments numériques mis à disposition sur le marché européen. Il sera entièrement applicable à partir du 11 décembre 2027.

Ce règlement impose des obligations de cybersécurité aux fabricants, importateurs et distributeurs desdits produits, dès la conception et tout au long du cycle de vie des produits. L'objectif est de garantir que les produits tels que les caméras domotiques, les téléviseurs, les jouets, les cartes à puce, les ordinateurs, les téléphones portables ou bien encore les systèmes de contrôle industriels, soient sécurisés. Le CRA améliore également la transparence pour les consommateurs, en permettant aux utilisateurs d'accéder aux informations sur la sécurité des produits qu'ils achètent et utilisent.

Il introduit un dispositif de surveillance de marché assuré, pour la France, par l'Agence nationale des fréquences (ANFR) avec le soutien de l'ANSSI. Les entreprises qui ne respecteraient pas leurs obligations prévues par le CRA s'exposeraient à des sanctions pouvant aller jusqu'au retrait du marché du produit ou des amendes, d'un montant maximum de 15 millions d'euros ou 2,5 % du chiffre d'affaires annuel mondial du fabricant. En 2025, un travail entre l'ANFR et l'ANSSI a été initié pour préparer la mise en œuvre de la réglementation. L'ANSSI assure le rôle d'autorité notifiante au titre du CRA en charge d'évaluer, de contrôler et de notifier les organismes d'évaluation de la conformité exerçant dans ce cadre. Ces organismes sont chargés de l'évaluation des produits les plus sensibles selon des procédures définies par le CRA. Ils devront être notifiés par l'ANSSI sur la base d'une accréditation par le Comité français d'accréditation (COFRAC). L'Agence a également un rôle de soutien technique auprès de l'ANFR, tant dans la définition de la stratégie de surveillance, que dans les contrôles menés par les laboratoires accrédités auxquels a recours l'ANFR. Elle construit en lien avec le COFRAC, un programme de notification.

Le règlement entrera en application progressivement entre juin 2026 et décembre 2027. Dans cette perspective, des travaux législatifs sont en cours. Le texte est d'application directe mais il nécessite l'adoption de plusieurs mesures visant à adapter le droit national à ce nouveau cadre, comme l'adaptation de l'article L.2321-4-1 du code de la défense issu de la loi de programmation militaire de 2024, qui prévoit un dispositif de notification des vulnérabilités par les éditeurs de logiciels ; ces derniers étant désormais soumis aux obligations du CRA en la matière.

Au cours de l'année écoulée, l'ANSSI a également participé à la comitologie des textes secondaires au niveau européen. Cette comitologie s'applique lorsque des compétences d'exécution sont conférées à la Commission européenne dans le cadre d'un acte législatif. Cet acte stipule que la Commission doit être assistée par un comité lorsqu'elle définit les mesures contenues dans l'acte d'exécution correspondant. L'Agence s'implique aussi dans les travaux de normalisation qui vont définir les exigences pour la mise en œuvre du texte.

Par ailleurs, l'Agence a été particulièrement mobilisée pour définir l'articulation du CRA avec les autres réglementations en lien avec la cybersécurité (Règlement sur l'intelligence artificielle, Règlement sur la cyber-résilience, NIS 2).

Enfin, en 2025, l'ANSSI a suivi les travaux liés à la gestion des vulnérabilités. En France, l'Agence est le CSIRT (Centre de réponse aux incidents cyber) coordinateur, c'est-à-dire le CSIRT qui coordonne et réceptionne pour la France les remontées de vulnérabilités effectuées via la plateforme unique de notification de l'Union européenne (UE). À ce titre, elle assurera la gestion des vulnérabilités au niveau national en centralisant les signalements de vulnérabilités. Dans cette perspective, l'ANSSI a suivi le projet de plateforme européenne de centralisation des vulnérabilités (EUVDB), mis en œuvre par l'Agence de l'Union européenne pour la cybersécurité (ENISA). Cette plateforme recueillera les signalements des vulnérabilités activement exploitées et des incidents graves ayant des répercussions sur la sécurité de produits, qui seront rendus obligatoires pour les éditeurs à compter du 11 septembre 2026. ●

# Le règlement sur la cybersécurité, cadre européen de certification de confiance

Le règlement sur la cybersécurité (*Cybersecurity Act*) définit un cadre de certification de cybersécurité pour harmoniser à l'échelle européenne les méthodes d'évaluation et les différents niveaux d'assurance de la certification.

Publié en 2019, c'est en 2025 que la pleine mise en œuvre d'un cadre de certification unifié à l'échelle européenne s'est concrétisée avec un premier schéma de certification européen bénéficiant d'une reconnaissance mutuelle au sein de l'UE, le schéma EUCC (*EU Common Criteria*).

Le schéma européen de certification selon les critères communs (ou schéma EUCC) est entré en vigueur en février 2024 dans le cadre de la mise en œuvre du CSA (Cybersecurity Act). Il vise à garantir que les produits des technologies de l'information et de la communication tels que les composants technologiques, le matériel et les logiciels, répondent à des normes de sécurité strictes. Le but : renforcer la cybersécurité et garantir la cohérence des approches dans l'ensemble de l'Union européenne.

Dans ce cadre réglementaire, l'ANSSI est l'autorité nationale de certification de cybersécurité, à double titre. D'une part, le Centre de certification national (CCN) de l'Agence est chargé de délivrer les certifications pour le niveau élevé du schéma EUCC. D'autre part, la Mission Contrôles et Supervision de l'ANSSI instruit, dans les cas où cela est nécessaire, notamment dans le schéma EUCC pour le niveau élevé, la procédure d'autorisation des organismes d'évaluation de la conformité, qui est un préalable à la délivrance des certificats.

Le CCN a reçu l'accréditation du COFRAC le 28 mars 2025, puis l'autorisation de l'ANSSI pour certifier les produits appartenant aux 3 domaines suivants :

- cartes à puce et dispositifs similaires ;
- dispositifs matériels avec boîtiers de sécurité ;
- produits réseaux ou logiciels génériques.

En parallèle, le centre d'évaluation de la sécurité (CESTI) *Serma Safety & Security*, avec lequel travaille le CCN, a lui-même été accrédité et autorisé à certifier les produits susmentionnés.

**Centre de certification français (CCN)**

**1er**

**émetteur de certificats CC (critères communs) dans le monde**

**73 certificats sur 313 émis**

Deux certificats EUCC ont ainsi pu être émis par l'ANSSI le 31 mars 2025. Ils sont les premiers certificats EUCC à être publiés dans l'Union européenne pour ce schéma de certification. Au total en 2025, une dizaine de certificats EUCC ont été émis au niveau européen dont 5 français.

Aujourd'hui, six centres d'évaluation français ont reçu l'autorisation par l'ANSSI pour travailler sur EUCC et ont été notifiés auprès de la Commission européenne, 5 pour le niveau d'assurance « élevé » et 1 pour le niveau « substantiel ».

Par ailleurs, une révision du CSA a été engagée en 2025, pour rationaliser les mesures de cybersécurité, renforcer la cyber-résilience et atteindre un niveau élevé de cybersécurité commun dans l'ensemble de l'UE, tout en contribuant au programme de simplification de la Commission européenne. L'ANSSI est pleinement engagée dans ces travaux qui doivent permettre de prendre en compte l'ensemble des risques de cybersécurité. ●

# Un cadre de confiance pour l'identité numérique : le règlement européen eIDAS

La résilience cyber, c'est aussi créer un cadre de confiance pour l'identité numérique et l'authentification, et faciliter la sécurité des transactions numériques transfrontalières. Des objectifs auxquels répond le règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, ou règlement eIDAS (*Electronic Identification, Authentication and Trust Services*).

L'adoption de la mise à jour du règlement eIDAS en 2024 a vu, notamment, l'apparition de portefeuilles européens d'identité numérique qui, à terme, seront accessibles à tous les citoyens et embarqueront diverses fonctionnalités, de l'authentification à des services en ligne à la signature électronique.

En 2025, l'ANSSI, en lien avec les autres acteurs de l'interministériel et sous l'impulsion de la Direction interministérielle du numérique (DINUM) en tant que cheffe de file, a participé activement aux négociations des actes d'exécution du règlement eIDAS relatif à ces portefeuilles et aux services de confiance. Le début d'année 2025 a notamment été marqué par l'adoption de 31 actes d'exécution pris en application du règlement eIDAS, qui encadrent la certification de ces portefeuilles électroniques européens.

Afin de pouvoir assurer son rôle d'autorité de certification des portefeuilles européens d'identité numérique, l'ANSSI a engagé les démarches d'accréditation auprès du COFRAC, pour répondre aux attentes de la réglementation et se préparer à la certification des solutions de portefeuille courant 2026.

Un portefeuille européen d'identité numérique devra être obligatoirement mis à disposition des citoyens par chaque État-membre. Il permettra notamment aux citoyens de s'identifier électroniquement avec un niveau de garantie élevé.

D'ici à la fin de 2026, chaque État devra proposer gratuitement au moins une solution de portefeuille électronique à ses citoyens. Les grandes plateformes du numérique devront permettre aux citoyens de s'authentifier via ces portefeuilles dès leur entrée en vigueur. Dès la fin de 2027, cette obligation concernera également les domaines des transports, de l'énergie, de la banque, des services financiers, de la sécurité sociale, de la santé, de l'eau potable, des services postaux, des infrastructures numériques, de l'éducation et des télécommunications. L'euro numérique devrait également reposer sur l'identification via les portefeuilles électroniques européens.

L'usage du portefeuille va donc progressivement se généraliser et le rôle de l'Agence consiste à certifier, au niveau de sécurité le plus élevé, les portefeuilles qui seront proposés par la France.

D'autres actes d'exécution sont attendus en 2026. En parallèle, l'ANSSI est investie dans les travaux de normalisation autour du règlement eIDAS, ce qui permet d'assurer la maîtrise des exigences applicables aux prestataires de services de confiance tout en garantissant la simplification réglementaire dans ce domaine. ●

**↘ Échange avec Matthieu Autret et Agate Rossetti, Chef et Cheffe adjointe de la Mission Contrôles et Supervision de l'ANSSI :**

***Quel est le rôle de la Mission Contrôles et Supervision au sein de l'ANSSI ?***
→ **Agate Rossetti :** La Mission Contrôles et Supervision assure des fonctions de supervision et de contrôle qui reviennent à l'ANSSI dans son rôle d'autorité compétente au titre de certaines réglementations européennes et nationales. Parmi celles-ci, on trouve notamment : la directive NIS 2 et les règlements CSA et eIDAS au niveau européen, et le dispositif SAIV, les autorisations, certifications, qualifications et agréments au niveau national. Du fait de la nature des activités concernées, elle est séparée fonctionnellement des fonctions d'accompagnement et de conseil de l'Agence. Elle se prépare, dans le contexte de la finalisation des cadres législatifs et réglementaires correspondants, à réaliser des procédures de contrôle visant à constater d'éventuels manquements dans le respect des droits des entités contrôlées. À l'issue d'une phase d'instruction, elle sera amenée à proposer les décisions qui en découlent, puis en assurera le suivi.

***Quelles décisions peuvent être prises à l'issue de l'instruction des procédures de contrôle ?***
→ **Matthieu Autret :** Ces décisions peuvent tout simplement prendre la forme d'une clôture du contrôle si la situation est jugée satisfaisante, ou bien de mesures d'exécution imposées aux entités pour corriger une situation non satisfaisante au regard de leurs obligations ou encore, si cela est nécessaire, d'une saisine de l'organe compétent pour prononcer d'éventuelles sanctions qui sera instauré par le législateur, et qui en l'état des travaux parlementaires, devrait être une commission indépendante de l'ANSSI, rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN) et composée de magistrats et de personnalités qualifiées.

***La Mission Contrôles et Supervision travaille-t-elle avec d'autres autorités de contrôle françaises ou européennes ?***
→ **Agate Rossetti :** Absolument.
D'une part elle doit jouer le rôle d'interface avec les autorités de supervision et de contrôle des autres États-membres de l'Union européenne, dans le cadre des coopérations prévues par les textes dans le champ de la cybersécurité et du partage de pratiques en vue de leur harmonisation.
D'autre part, elle occupe ce même rôle avec d'autres autorités de contrôle nationales avec lesquelles une coordination est nécessaire, compte-tenu de la complémentarité des champs de compétences (Commission nationale de l'informatique et des libertés [CNIL], Autorité de contrôle prudentiel et de résolution [ACPR], Autorité des marchés financiers [AMF], etc.). ●

# Le développement d'une offre de services de cybersécurité

## Offre de services : démultiplier l'accompagnement cyber

L'ANSSI a œuvré, en 2025, à la construction de services numériques innovants afin de répondre aux besoins croissants de ses bénéficiaires, entités publiques et entreprises. L'offre de services se décline ainsi en plusieurs plateformes qui accompagnent un changement d'échelle nécessaire à la mise en œuvre de ses nouvelles missions.

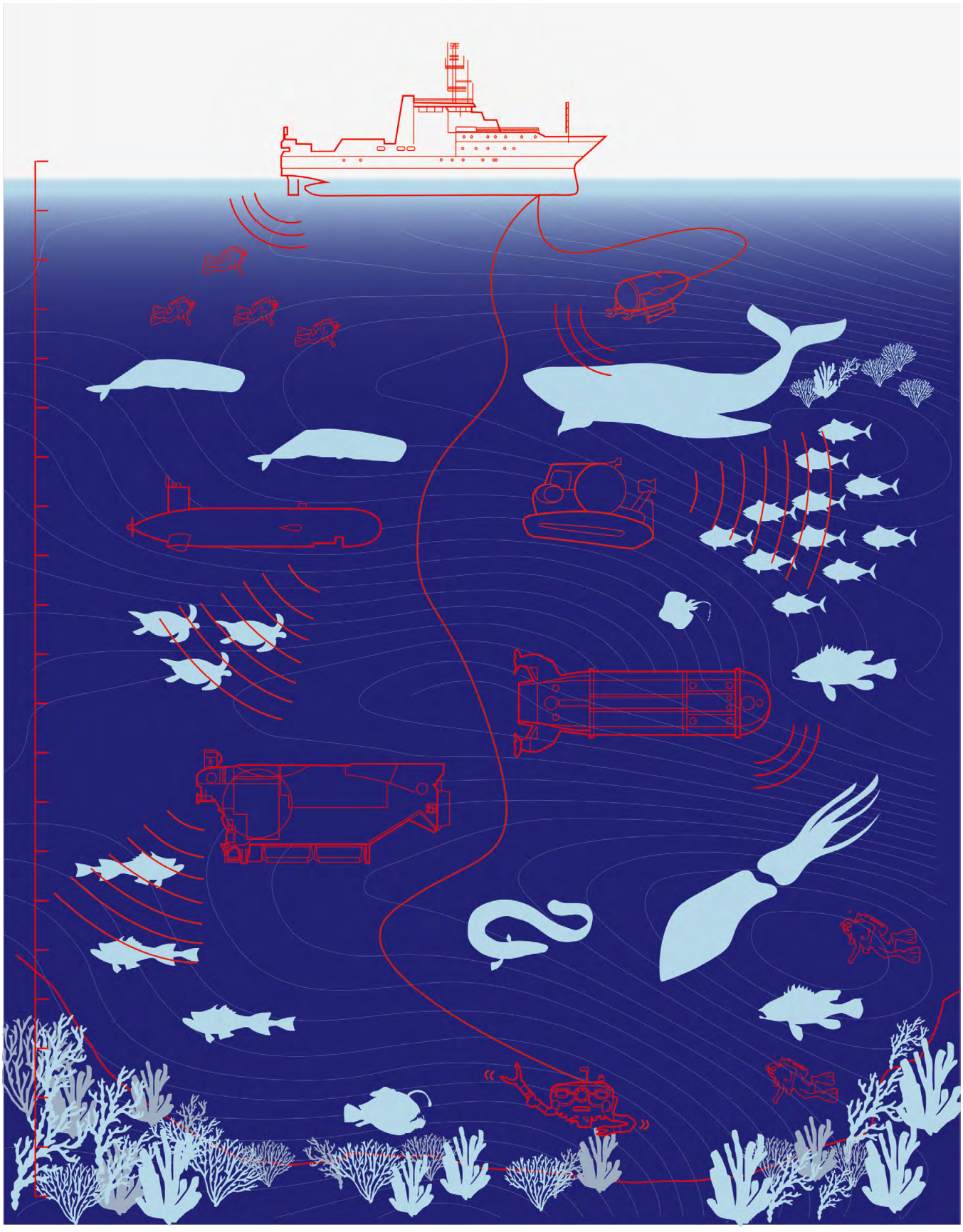
Ces outils permettent d'amplifier les actions de l'Agence, via des canaux différents, en favorisant l'usage en autonomie par les bénéficiaires des ressources, et en proposant des parcours et contenus au plus proche de leurs besoins.

L'ANSSI bénéficie également de partenariats externes importants pour penser et déployer ses services, avec le réseau Beta Gouv, l'Agence nationale de la cohésion des territoires (ANCT) et le ministère de l'Éducation nationale. En mars 2025, MonServiceSécurisé, l'outil de la mise en conformité avec la réglementation cyber pour les entités publiques, a été désigné service à impact national par la DINUM. MonServiceSécurisé a ainsi rejoint le club restreint des 30 services les plus impactants créés par les incubateurs de l'État.

En avril 2025, l'Agence a lancé MesServicesCyber. MesServicesCyber est la plateforme numérique de l'ANSSI pour aider l'ensemble des organisations publiques et privées à renforcer leur cybersécurité, en facilitant l'accès à des services et à de nombreuses ressources utiles adaptés aux besoins de chaque organisation (outils, guides, contacts, prestataires, financements cyber) ainsi qu'à une démarche de sécurisation : un test de maturité cyber en 3 minutes, ainsi que le diagnostic Cyberdépart. Il s'agit d'un diagnostic de premier niveau gratuit et accompagné, destiné aux organisations les moins matures. MesServicesCyber s'adresse, en particulier, aux entités qui seront régulées par la directive NIS 2, que la plateforme vise à accompagner dans leur montée en maturité. Elle dispose d'un espace dédié proposant notamment un outil de comparaison entre le Référentiel Cyber France (ReCyF) et d'autres référentiels de sécurité.

« Face à la menace cyber et à la nécessité pour les administrations et les entreprises d'agir pour leur cybersécurité, la plateforme *MesServicesCyber* a pour vocation de répondre à leurs besoins. »

Jean-Baptiste Demaison
Responsable du Laboratoire d'innovation publique de l'ANSSI



**+ de 20 000**
**ressources consultées sur MesServicesCyber**

**+ de 9 900**
**tests de maturité cyber réalisés**

**+ de 5 500**
**organisations ayant réalisé leur diagnostic Cyberdépart**

Par ailleurs, en 2025, JeCliqueOuPas, le service en ligne d'analyse de fichiers à destination des agents de l'État, a été ouvert aux connexions via ProConnect, et à l'utilisation par API (*Application Programming Interface*, interface qui permet à différentes applications ou systèmes de communiquer entre eux en échangeant des données ou des fonctionnalités). Il est utilisé par plusieurs ministères et intégré sur des services numériques de la DINUM comme France Transfert.

**+ de 50**
**nouvelles entités bénéficiaires**

**+ de 300**
**entités bénéficiaires au total**

**+ de 10 millions**
**de fichiers analysés**

Dans une démarche d'amélioration continue, le site de l'ANSSI, cyber.gouv.fr, et le site du CERT-FR, cert.ssi.gouv.fr, site de l'entité gouvernementale et nationale assurant la mise en œuvre opérationnelle de la fonction d'autorité de défense des systèmes numériques d'intérêt pour la Nation dévolue à l'ANSSI, ont évolué en 2025 pour mieux répondre aux besoins des utilisateurs et optimiser le parcours jusqu'aux contenus recherchés. Le site de l'ANSSI met à disposition toute l'information institutionnelle de l'Agence : ses missions, son actualité, ses principales publications, ou encore ses postures sur les grands enjeux technologiques. Le site du CERT-FR permet de consulter les informations relatives à la connaissance de la menace, à la détection, ou encore à la réponse aux incidents. Les guides et les outils de l'ANSSI ont migré vers MesServicesCyber.

## Le développement des CSIRT pour changer d'échelle

Maillons essentiels du dispositif d'accompagnement de proximité, les centres de réponse à incident cyber, dits CSIRT, participent à renforcer les actions de prévention, de détection et d'assistance dans les territoires et au sein des secteurs et des ministères.

Les différents CSIRT sont amenés à échanger continuellement des informations et des retours d'expérience afin de maintenir un bon niveau de confiance et de coopération, d'améliorer la connaissance de l'état de la menace et de mieux assister leurs bénéficiaires. Les échanges de l'ANSSI avec l'écosystème français de CSIRT se sont fortement accrus en 2025, tant en matière opérationnelle que capacitaire, avec notamment le partage d'outils et de méthodes de réponse à incident ou de connaissance de la menace. En 2025, 366 incidents ont été relayés du CERT-FR vers les CSIRT territoriaux.

Au cours de l'année, l'ANSSI a également activement soutenu le projet porté par le groupement d'intérêt public Action contre la Cybermalveillance (GIP ACYMA), d'intégration des CSIRT territoriaux dans le parcours du 17Cyber, service public d'assistance en ligne destiné aux particuliers, entreprises, associations et collectivités victimes de cybermalveillance, concourant à l'objectif d'un parcours victime simple et lisible.

Enfin, l'année 2025 a permis le lancement de l'appel à manifestation d'intérêt pour le renforcement de l'accompagnement local aux enjeux de cybersécurité (AMI-RALEC), qui prolonge l'action de l'ANSSI, entreprise dès 2021. Sur les 74 dossiers reçus, l'Agence en a sélectionné 17 pour un montant total de subvention de 6,8 millions d'euros (400 000 euros par projet). Cette initiative aura notamment permis la création de futurs centres de réponse à incident cyber en Auvergne-Rhône-Alpes et sur le territoire de Mayotte.

En 2025, l'ANSSI a eu 676 interactions avec l'écosystème des CSIRT territoriaux, sectoriels et ministériels, notamment :

- 375 points de synchronisation opérationnels (partages sur les incidents, la menace, la détection) ;
- 28 comités techniques permettant d'animer une communauté et d'initier des projets communs ;
- 49 échanges bilatéraux ;
- 221 partages de productions (indicateurs de compromission, états de la menace sectoriels, fiches rançongiciels, signalements de vulnérabilités, points de situation opérationnels, rapports d'activité, etc.).

## France Relance et France 2030 : des effets tangibles pour la cybersécurité

Pour répondre à une menace devenue systémique, un programme de parcours de cybersécurité a été déployé pendant plus de quatre ans. Volet cybersécurité du plan France Relance, qui a pris fin en 2025, ces parcours avaient pour objectif d'élever la sécurité numérique des services publics, de dynamiser l'industrie de cybersécurité française et européenne et de favoriser des investissements durables au service de la cybersécurité des organisations. Avec 100 millions d'euros, le programme des parcours de cybersécurité a constitué un investissement sans précédent.

**945**
**entités ont bénéficié de cet accompagnement, dont :**

**707** collectivités territoriales

**134** établissements de santé

**87** autres établissements publics

**17** centres de recherche et d'enseignement supérieur

**Parmi celles-ci, 62 entités ont été accompagnées dans les territoires d'outre-mer**

Ces parcours ont permis d'élever le niveau de cyberdéfense des bénéficiaires de manière significative : en moyenne, les bénéficiaires sont passés d'un score de maturité cyber de D+ à B, soulignant un progrès conséquent. Ils laissent un héritage exploitable dans la durée, dans la perspective notamment de la mise en œuvre de NIS 2, avec la mise à disposition d'outils et de méthodes adaptés aux besoins de chaque bénéficiaire.

Le programme a également permis de dynamiser l'offre industrielle de cybersécurité dans les territoires et de renforcer l'offre française et européenne.

**197**
**prestataires présents sur l'ensemble du territoire national impliqués**

**40**
**millions d'euros**
**dédiés à l'acquisition de produits de cybersécurité français et européens (dont 33 millions d'euros pour des produits français)**

**16,7 M €**
**mobilisés par l'ANSSI pour renforcer la cybersécurité, dont :**

**9,1 M €**
**pour l'acquisition de logiciels**

**3,9 M €** **pour l'achat de matériel plus performant et sécurisant de type EDR**

**3,7 M €** **pour recourir à de la prestation d'aide au déploiement chez les bénéficiaires les plus fragiles**

En 2025, l'ANSSI a aussi contribué à différents dispositifs dans le cadre de France 2030, plan d'investissement de 54 milliards d'euros pour permettre de rattraper le retard industriel français, et d'investir massivement dans les technologies innovantes. Elle participe par ailleurs à la gouvernance du programme en étant représentée au Comité de pilotage ministériel opérationnel numérique qui valide les cahiers des charges et les projets financés pour l'ensemble des stratégies liées au numérique.

En dehors de la stratégie d'accélération cybersécurité de France 2030, l'ANSSI est investie dans la stratégie *cloud*, avec comme objectif la montée en maturité cyber des offres *cloud* des acteurs français. L'Agence participe également à la stratégie sur l'intelligence artificielle (IA), en intégrant des critères de maturité cyber dans les appels à projets.

En 2025, l'ANSSI a joué un rôle clé dans le lancement de la 4e vague de l'appel à projets « Développement de technologies innovantes critiques » (DTIC) par le Secrétariat général pour l'investissement (SGPI) qui permet de cofinancer des projets de recherche et développement portant sur des briques technologiques innovantes et critiques en cybersécurité. L'Agence a contribué à la sélection des thématiques d'intérêt du cahier des charges et à la sélection des projets, notamment afin de s'assurer de la bonne adéquation des thématiques financées avec les besoins du marché.

# Renforcer le développement d'offres de cybersécurité de confiance

L'ANSSI accompagne l'écosystème des éditeurs de produits et prestataires de services de cybersécurité afin de veiller à l'existence d'une offre cyber de confiance sur le marché. Cet accompagnement passe par un suivi actif des entreprises de cybersécurité. 2025 a permis à l'Agence de poursuivre un projet étendu de prospection et de diagnostic le plus exhaustif possible, de l'écosystème des prestataires de cybersécurité.

L'animation des communautés d'offreurs qualifiés par l'ANSSI a continué à monter en puissance, avec l'aboutissement de plusieurs livrables co-construits avec ces communautés (nouvelle portée « gestion de crise » du référentiel sur les prestataires de réponse aux incidents de sécurité (PRIS), corpus doctrinal sur la supervision, etc.), et à travers l'inclusion de nouveaux acteurs au sein des ateliers, tels les prestataires de service *cloud* et les éditeurs de produits de supervision. Cette animation de communautés permet de favoriser le partage de connaissances et la montée en compétences des acteurs impliqués.

En janvier 2025, pour lever certaines complexités remontées par le terrain, l'Agence a initié un chantier de mise à jour du référentiel sur les prestataires de détection d'incidents de sécurité (PDIS). Celui-ci a déjà mené à la publication d'un addendum au référentiel PDIS. Cette première publication a officiellement lancé de manière concrète le chantier de mise à jour du référentiel, actuellement en cours.

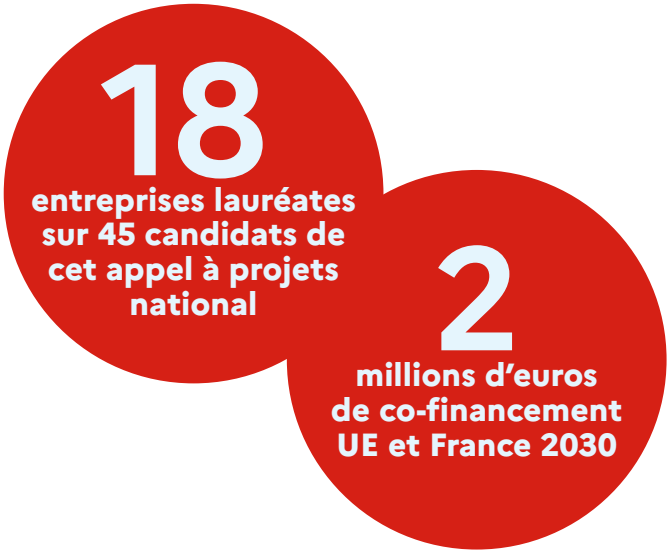
À la suite d'un appel à commentaires, le référentiel PRIS a également été mis à jour en octobre 2025. Il intègre désormais l'activité de gestion de crise cyber. Ces évolutions illustrent le dynamisme des référentiels de l'ANSSI, qui s'adaptent aux réalités du terrain et de la menace.

Afin de rendre visibles les dispositifs financiers européens pouvant bénéficier aux organisations du domaine de la cybersécurité (programmes *Digital Europe* et *Horizon Europe*), de lancer des dispositifs de soutien financier à l'échelon national pour l'écosystème de la cybersécurité, et d'animer la communauté cyber française, le Centre de coordination cyber français (NCC-FR), incarné par l'ANSSI, a poursuivi en 2025 son travail avec le réseau de NCC dans les États-membres de l'UE et le Centre de compétences cyber européen (ECCC).

Ensemble, l'ECCC et le réseau des NCC visent à renforcer l'autonomie stratégique de l'UE avec des investissements conjoints dans des projets stratégiques de cybersécurité. L'ECCC élabore et met en œuvre, avec les États-membres, et l'écosystème de la cybersécurité, un programme commun pour le développement des capacités de cybersécurité européennes et leur large déploiement dans les domaines d'intérêt public et dans les entreprises, en particulier les PME.

Le NCC-FR, hébergé par l'Agence et co-financé par l'UE, est dans une phase d'opérationnalisation de 24 mois ; sa revue de mi-parcours a eu lieu en 2025.

En janvier 2025, le NCC-FR a clôturé l'appel à projets national « Soutien aux PME et startups pour renforcer leurs compétences dans le domaine de la cybersécurité », lancé conjointement par l'ANSSI, le NCC-FR, le SGPI et Bpifrance. Les projets financés ont eu une durée de 6 à 8 mois et se sont clôturés en fin d'année 2025.




Par ailleurs, tout au long de l'année 2025, le NCC-FR a activement relayé, auprès de l'écosystème cyber français, les dispositifs de soutien financiers européens des programmes *Horizon Europe* et *Digital Europe*.

Le 14 avril 2025, le NCC-FR et la Direction générale des entreprises (DGE) ont organisé l'événement « Info Day », pour présenter les appels à projets du programme *Digital Europe*. Le 4 août 2025, le NCC-FR a lancé un appel à manifestation d'intérêt relatif à l'appel à projets « Outils de cybersécurité, technologies et services reposant sur l'IA » du programme *Digital Europe*, afin de mobiliser l'écosystème sur ce sujet technologique clé. L'ANSSI a ensuite organisé un atelier collaboratif qui a réuni 30 industriels de la cybersécurité intéressés autour de cas d'usage et a facilité la préfiguration de candidatures françaises à cet appel à projets européen.

Enfin, le NCC-FR a préparé en 2025 un nouvel accord de subvention entre l'Agence et l'ECCC pour le passage à l'échelle de ses services dans un groupement partenarial élargi avec un budget total de 10 854 942 euros pour la période 2026-2029. Cet accord de subvention sera accompagné d'un accord de consortium pour agrandir le consortium actuel avec le Campus Cyber, le Campus Cyber Bretagne, Paris Systematic, Aktantis et Bpifrance. ●

# La coopération cyber européenne et internationale, au cœur des priorités

## Renforcer les échanges opérationnels grâce aux réseaux de coopération européens

Réseau des CSIRT européen, le *CSIRT Network* a prouvé en 2025 sa capacité à s'activer en permettant aux partenaires des 27 États-membres d'échanger lors des différents cas de vulnérabilités ayant engendré des impacts à l'international. Il a également facilité la communication en cas d'incidents cyber transfrontaliers.

L'ANSSI, par le CERT-FR, s'est pleinement impliquée au sein du *CSIRT Network* en 2025, en partageant de l'information notamment sur certains incidents et sur certaines campagnes d'attaques. Elle a, entre autres, animé le groupe chargé de l'évaluation de la maturité des CSIRT.

L'Agence a également continué à porter des propositions structurantes au sein du réseau, visant à encourager le partage d'informations dans des phases pré-crise. L'ANSSI a notamment joué un rôle déterminant dans la révision du *Cyber Blueprint*, plan européen de gestion des crises cyber. Cette actualisation vise à renforcer la coordination entre les États-membres, notamment au travers du réseau CyCLONe (*Cyber Crisis Liaison Organisation Network*, réseau qui rassemble les agences en charge de la gestion de crise de cybersécurité) et du *CSIRT Network*, afin d'assurer une réponse rapide, structurée et efficace aux crises cyber majeures. CyCLONe complète les structures de cybersécurité existantes au niveau de l'UE en établissant un lien entre la coopération au niveau technique et au niveau politique. Le réseau contribue à la mise en œuvre du plan d'action de la Commission européenne pour une réaction rapide en cas d'incident ou de crise de cybersécurité transfrontière de grande ampleur. L'Agence a contribué à positionner CyCLONe comme l'acteur central de la gestion opérationnelle des crises cyber à l'échelle européenne, consolidant ainsi la résilience collective de l'UE.

En novembre 2025, dans le cadre de la mise à l'épreuve de ce nouveau plan, l'ANSSI a participé à l'exercice de crise BlueOLEx25, qui visait à tester les capacités des responsables européens de gestion de crise cyber et à renforcer la coopération entre les acteurs impliqués. ●

## Une coopération internationale accrue dans les différents champs de la cybersécurité

Au-delà du *CSIRT Network* et de CyCLONe, la coopération européenne et internationale a porté en 2025 sur divers champs de la cybersécurité.

La coopération franco-allemande s'inscrit spécifiquement dans une volonté commune de renforcer l'autonomie numérique européenne. La déclaration commune de l'ANSSI et de son homologue, le *Bundesamt für Sicherheit in der Informationstechnik* (BSI), en marge du sommet franco-allemand sur la souveraineté numérique en novembre 2025, témoigne d'une prise de conscience commune des menaces liées à l'évolution du contexte international et de la nécessité de promouvoir une approche européenne robuste.

La coopération franco-allemande permet, d'une part, le partage de bonnes pratiques et l'organisation régulière d'ateliers d'experts (*cloud,* intelligence artificielle et menace en 2025). D'autre part, cette coopération vise à harmoniser les positions vis-à-vis des réglementations européennes et nationales.

Au-delà de l'Allemagne, l'Agence a poursuivi en 2025 son travail d'accompagnement et d'échange avec l'ensemble des autres pays européens. D'une part, la contribution à des documents de position (*position papers*) italien (services *cloud*), belge et néerlandais (révision du CSA) a permis de faire rayonner les positions françaises sur divers sujets européens en lien avec la cybersécurité. D'autre part, une véritable dynamique d'échanges opérationnels a été mise en place avec la Pologne, l'Irlande, le Danemark, la Suisse et la Moldavie sur l'analyse de la menace afin d'accompagner certains partenaires dans leur montée en compétence et d'ouvrir la porte à une collaboration plus approfondie avec d'autres. Enfin, l'appui apporté à l'*Agenzia per la Cybersicurezza Nazionale* (ACN) quant à la préparation des Jeux olympiques et paralympiques d'hiver de Milan-Cortina de février 2026 a permis de promouvoir les bonnes pratiques françaises auprès de ce partenaire.

La coopération cyber sur le plan opérationnel spécifiquement, a permis le bon déroulé du second volet de l'opération de coopération judiciaire internationale ENDGAME, qui a eu lieu en mai et novembre 2025. Cette opération de démantèlement vise à lutter contre la cybercriminalité internationale. Les autorités allemandes, danoises, françaises, néerlandaises, américaines, australiennes et britanniques ont coopéré pour aider à la compréhension des réseaux ou des codes malveillants, mener des actions de démantèlement des infrastructures et élaborer les stratégies d'assistance aux victimes identifiées. Dans le cadre de cette opération, l'ANSSI a apporté son soutien pour l'identification et la notification des victimes, et a partagé des recommandations de sécurité dans le cadre de l'assistance aux victimes identifiées, afin de limiter les conséquences d'une infection avérée.

L'Agence a également participé à l'édition 2025 de l'exercice international de cyberdéfense *Locked Shields*, qui s'est déroulée du 28 avril au 9 mai 2025 dans les locaux de l'École des ingénieurs en intelligence informatique (EPITA). L'exercice a rassemblé 4 000 spécialistes en cyberdéfense et lutte offensive provenant de diverses organisations issues de 41 nations. L'équipe franco-polonaise, composée d'agents du Commandement de la cyberdéfense (COMCYBER) du ministère des Armées, de l'ANSSI, du Commandement Cyber polonais et des étudiants de quatre écoles partenaires (l'EPITA, l'ENSIBS, l'École 2600, l'ESGI) s'est hissée à la deuxième place du podium. Tant au niveau européen qu'international, *Locked Shields* 2025 a permis de renforcer la capacité de la France à travailler avec ses alliés. ●

« Il est illusoire de croire à des frontières dans le cyberespace. C'est à nous de prendre en compte les mutations rapides de notre environnement géopolitique pour assurer notre cyberdéfense. C'est pourquoi l'ANSSI travaille avec l'ensemble de ses partenaires européens et internationaux pour avancer dans une logique partenariale et relever collectivement les défis. »

Catherine Poupon
Cheffe de la Division Coordination Internationale de l'ANSSI

## ↘ REMPAR25, un exercice de crise d'ampleur inédite pour s'entraîner collectivement

Le 18 septembre 2025, l'ANSSI a organisé l'exercice de crise massifié REMPAR25, avec le soutien du Campus Cyber national, du Club de la continuité d'activité (CCA), du Club de la sécurité de l'information français (CLUSIF), du Club des experts de la sécurité de l'information et du numérique (CESIN), et plus d'une cinquantaine d'autres partenaires sur tout le territoire national. L'objectif était d'évaluer et renforcer la capacité collective de la France à affronter un scénario de black-out numérique d'ampleur inédite.

Deux modalités de participation étaient proposées aux participants à l'exercice : une immersion en interne, au sein de leur propre organisation, ou une intégration à une cellule de crise fictive, dans l'un des 19 sites d'accueil répartis sur tout le territoire. Dirigeants, experts du numérique, juristes, responsables des ressources humaines et communicants ont ainsi testé en conditions réelles leur capacité à réagir, coordonner et décider sous pression. REMPAR25 a simulé une crise cyber systémique, entraînant une interruption massive des services numériques essentiels. Pour la première fois, entreprises, administrations et acteurs territoriaux ont pu s'immerger dans une crise cyber majeure, révélant l'importance cruciale des plans de continuité d'activité. Un kit complet de l'exercice, incluant le scénario détaillé, les retours d'expérience et les bonnes pratiques, a été mis à disposition à l'issue de l'exercice pour permettre à chaque organisation de s'entraîner.

Dans le cadre de la Revue nationale stratégique 2025, cet exercice massifié a constitué un premier baromètre du niveau de préparation de la Nation à une gestion de crise d'origine cyber d'ampleur. Il a souligné l'importance de la coordination entre les différents niveaux de réponse : local et national. REMPAR25 a également permis de préparer les organisations à l'arrivée de la transposition de la directive NIS 2, qui recoupe des objectifs de gestion de crise. L'emploi du formulaire de déclaration d'incidents de l'ANSSI dans le cadre de l'exercice a également permis de tester sa bonne compréhension et son traitement à large échelle par les organisations participantes. Pour 95 % des participants, REMPAR25 a été l'occasion de mettre en place, à l'issue de l'exercice, des actions en matière de gestion de crise et/ou de sécurité des systèmes d'information. ●

« Ce scénario de *black-out* numérique, qui fait la particularité des exercices de crise REMPAR, a révélé l'importance cruciale des plans de continuité d'activité, et la nécessité pour chaque organisation d'intégrer la gestion de crise d'origine cyber dans sa stratégie, de manière proactive et collaborative avec l'ensemble des fonctions de l'organisation. »

Sarah Atakou-Gauthierot
Cheffe du Bureau Management des Crises Cyber de l'ANSSI

## ↘ Le partage de connaissances pour s'adapter aux évolutions de la menace cyber

Le CERT-FR étudie la menace cyber portant sur les systèmes d'information les plus critiques de la Nation mais également sur l'écosystème national de manière plus générale. Le *Panorama de la cybermenace 2024*, publié en mars 2025, a été l'occasion pour l'ANSSI de revenir sur les grandes tendances de la menace informatique ainsi que sur les éléments et incidents marquants dont elle a eu connaissance en 2024, année d'organisation des Jeux olympiques et paralympiques en France.

Au cours de l'année 2025, l'Agence a également publié de nombreux états de la menace pour sensibiliser largement et adresser des recommandations adaptées (voir la bibliographie en fin de rapport d'activité). En complément, le CERT-FR a régulièrement partagé des informations à caractère opérationnel (indicateurs de compromission, rapports d'analyse, etc.) au sein de l'écosystème national et avec ses partenaires internationaux. Ce partage d'informations au niveau national se fait notamment dans le cadre du Centre de coordination des crises cyber (C4).

Placé sous l'égide du SGDSN, le C4 est composé de l'ANSSI, du COMCYBER, de la Direction générale de l'Armement (DGA), de la Direction générale de la Sécurité extérieure (DGSE), de la Direction générale de la Sécurité intérieure (DGSI) et du ministère de l'Europe et des Affaires étrangères. Il assure une activation coordonnée et pertinente des leviers d'action face aux cyberattaques et propose des stratégies de réponse à l'autorité politique.

Le 29 avril 2025, la France a, pour la première fois, par la voix de son ministre de l'Europe et des Affaires étrangères, attribué de manière publique, un ensemble de cyberattaques au renseignement militaire russe (GRU). Cette attribution a été portée par un ensemble de publications simultanées, dont la publication par l'ANSSI sur le « ciblage et la compromission d'entités françaises au moyen du mode opératoire d'attaque APT28 » qui revient sur des attaques informatiques observées par l'Agence et ses partenaires du C4. Le mode opératoire d'attaque APT28 a été utilisé contre de nombreuses entités en France, en Europe, en Ukraine et en Amérique du Nord, afin de collecter des renseignements. En 2024, la victimologie française des campagnes associées à APT28 comprenait des entités des secteurs gouvernemental, diplomatique et de la recherche. Les investigations menées par l'ANSSI et ses partenaires du C4 ont permis d'identifier plusieurs chaînes d'infection, présentées dans le document. ●

« Le partage de connaissances sur la menace est un outil efficace pour sensibiliser un large public à la réalité de la menace cyber. Cela contribue aussi à aider l'ensemble des écosystèmes à mieux se protéger face à différents types d'acteurs malveillants aux motivations variées comme l'espionnage, la recherche de gain financier ou la déstabilisation. »

Émilie Nodet
Cheffe de la Division Connaissance et Anticipation de l'ANSSI

# Se préparer aux transformations et aux ruptures technologiques

L'intelligence artificielle et l'arrivée d'un ordinateur quantique d'une puissance suffisante pour mettre à mal les mécanismes de cryptographie qui protègent actuellement notre vie numérique, ont été l'objet de nombreux travaux menés par l'ANSSI en 2025. L'objectif est de se préparer et de maîtriser les transformations et ruptures que peuvent représenter ces technologies.

# Accompagner le développement de l'intelligence artificielle

L'ANSSI travaille sur l'IA depuis 2017, principalement au travers de travaux de recherche sur la détection. Face au déploiement croissant de ces technologies dans les systèmes d'information et au progrès de ces technologies, l'Agence a élargi le périmètre de ses réflexions sur l'IA dès 2022, tant à des fins de sécurisation des systèmes d'IA que d'identification des opportunités offertes par ces technologies pour la cybersécurité.

L'IA soulève des enjeux de cybersécurité déclinés en trois catégories :

- La cybersécurité de l'IA : les systèmes d'IA présentent des vulnérabilités comme tout système d'information et peuvent faire l'objet d'attaques, appelant à leur sécurisation. Si nombre de mesures de sécurité s'appliquent, ces systèmes présentent des vulnérabilités spécifiques appelant à définir des doctrines de sécurisation qui leur sont adaptées ;
- La cybersécurité face à l'IA : les systèmes d'IA représentent des opportunités pour les cyberattaquants en termes d'automatisation des attaques, de personnalisation et de mutation de la menace, rendant toujours plus complexe la mise en œuvre d'une cybersécurité efficace ;
- La cybersécurité par l'IA : l'utilisation de l'IA est particulièrement prometteuse pour améliorer l'efficacité des dispositifs de cybersécurité.

L'ANSSI intègre ces différents enjeux de sécurité dans son plan d'action ; la priorité est toutefois donnée à la cybersécurité de l'IA.

Les travaux de l'Agence en matière d'IA s'articulent autour des axes prioritaires suivants :

- Participer à la construction de schémas de certification de cybersécurité de produits et de systèmes d'IA ;
- Accompagner les administrations dans leurs déploiements d'IA ;
- Développer les capacités de recherche de l'Agence ;
- Accompagner les offreurs et les acquéreurs de solutions de cybersécurité ;
- Sensibiliser l'ensemble de l'écosystème aux enjeux de cybersécurité liés à l'IA ;
- Suivre le développement de l'Institut national d'évaluation et de la sécurité de l'intelligence artificielle (INESIA) ;
- Accompagner la mise en œuvre du règlement sur l'IA (dit « RIA ») sur le volet cyber.

L'Agence s'inscrit dans la continuité de la stratégie nationale autour de l'IA portée par le gouvernement, dont l'objectif est de faire de l'IA un levier de compétitivité et d'indépendance au service du bien commun et d'utiliser cette technologie aux bénéfices de la cyberdéfense.

« En matière d'IA, notre rôle est d'apporter de la clarté, d'anticiper, de mesurer les risques comme les opportunités – le tout pour accompagner l'écosystème vers la promotion d'une IA à la fois sûre et résiliente. »

Hugo Mania
Chef de projet IA de l'ANSSI

## Le Sommet pour l'action sur l'IA : unir nos forces pour sécuriser l'intelligence artificielle

À l'occasion du Sommet pour l'action sur l'IA qui s'est tenu du 6 au 11 février 2025, l'ANSSI a publié une analyse de risques de haut niveau co-signée par 19 partenaires internationaux et 5 partenaires nationaux intitulée *Développer la confiance dans l'IA à travers une approche par les risques cyber*. Ce document met en évidence les risques cyber auxquels sont exposés les systèmes d'IA. Il relaie des recommandations stratégiques afin de favoriser une meilleure prise en compte de la cybersécurité dans le développement et l'intégration de ces systèmes. Les agences internationales et autorités gouvernementales cosignataires soutiennent l'usage des systèmes d'IA de confiance et souhaitent rendre plus sûre leur chaîne de valeur.

Le Sommet a également été l'occasion pour l'Agence d'organiser un exercice de crise cyber autour de l'IA le 11 février 2025, qui a mobilisé près de 200 participants, issus des domaines de l'IA et de la cybersécurité (fabricants, concepteurs de systèmes d'IA, experts en cybersécurité). L'exercice a permis d'identifier les bonnes pratiques en cas de cyberattaque affectant un système d'IA, de renforcer les échanges entre professionnels de l'IA et les experts en cybersécurité afin d'identifier les synergies entre les deux domaines, et d'identifier les besoins et opportunités de partage d'informations sur les vulnérabilités et incidents significatifs affectant les systèmes d'IA. Un kit d'exercice a été mis à la disposition de tous. En marge du Sommet, l'ANSSI a aussi organisé le 12 février 2025 un événement rassemblant les directeurs d'agences nationales de cybersécurité. Cet événement a permis d'échanger sur les modèles d'intégration de l'IA et sur les approches concrètes pour maîtriser les risques cyber liés à leur déploiement. Les échanges ont permis d'identifier des axes d'engagements internationaux que l'Agence promeut dans les enceintes multilatérales comme dans ses interactions bilatérales avec ses homologues, notamment dans la perspective de la présidence française du G7. ●

## L'ANSSI mobilisée à tous les niveaux pour une meilleure utilisation de l'IA

Si le Sommet pour l'action sur l'IA de février 2025 a permis d'attirer l'attention de l'écosystème et de le sensibiliser aux enjeux et risques de cybersécurité liés à ces technologies, l'ANSSI s'est également attachée tout au long de l'année à poursuivre ses travaux sur l'IA.

À la lumière de l'utilisation croissante des systèmes d'IA, l'écosystème français et européen doit travailler à la création de schémas de certification dédiés. Ces derniers sont nécessaires pour favoriser le développement et l'usage des systèmes d'IA de confiance sur le marché. L'Agence a travaillé en 2025, avec l'écosystème français et les partenaires étrangers, à l'élaboration de méthodes d'évaluation et de certification adaptées aux systèmes d'IA.

Le déploiement de l'IA dans les administrations, à des fins d'outillage ou d'expérimentation, a été une autre priorité en 2025 pour l'Agence, qui assure la cybersécurité de ces dernières. L'ANSSI a notamment accompagné le déploiement d'Albert, l'outil d'intelligence artificielle générative développé par la DINUM.

Les solutions de cybersécurité intégrant de l'IA se sont multipliées sur le marché en 2025. L'Agence contribue à accompagner les industriels dans l'intégration sécurisée de l'IA au sein des solutions de sécurité. En juillet 2025, l'ANSSI a notamment mené une étude de marché sur l'usage et les impacts potentiels de l'intelligence artificielle dans le domaine de la détection et de la réponse à incident cyber afin de développer sa connaissance des pratiques actuelles.

Plusieurs travaux de sensibilisation de l'écosystème aux enjeux de cybersécurité liés à l'IA ont aussi été menés en 2025. En particulier, une formation de « sensibilisation aux enjeux de cybersécurité liés à l'IA » sera proposée à partir de 2026 au Centre de formation à la sécurité des systèmes d'information (CFSSI) de l'ANSSI.

Enfin, l'Agence a participé à des projets de recherche et encadré plusieurs thèses sur la cybersécurité et l'IA, permettant ainsi de renforcer son expertise dans le domaine. Les travaux de préfiguration d'une implication plus large des laboratoires de l'ANSSI sur le sujet de la cybersécurité de l'IA ont démarré en 2025. ●

## Le Règlement européen sur l'intelligence artificielle et l'Institut national pour l'évaluation et la sécurité de l'intelligence artificielle, dispositifs clés pour une utilisation sûre de l'IA

Le règlement européen sur l'intelligence artificielle, également connu sous le nom d'*AI Act*, est le premier cadre législatif au monde qui encadre le développement, la mise sur le marché et l'utilisation des systèmes d'IA. Il est entré en vigueur le 1er août 2024. Ce texte établit des règles harmonisées dans l'ensemble de l'UE pour garantir que les systèmes d'IA respectent les droits fondamentaux, les valeurs européennes et les exigences de sécurité. Il s'appuie sur une approche basée sur les risques, catégorisant les systèmes d'IA selon leur impact potentiel, de risque minimal à inacceptable. En plus de protéger les citoyens et de limiter les usages nuisibles, le règlement encourage l'innovation, notamment pour les petites et moyennes entreprises (PME), et vise à renforcer la confiance dans ces nouveaux usages en pleine expansion.

L'ANSSI s'est impliquée en 2025 dans la mise en œuvre du RIA sur le volet cybersécurité, orienté sur la surveillance de marché. Le RIA introduit notamment une obligation pour les États-membres de mettre en place un schéma de gouvernance visant à accompagner l'entrée en vigueur du texte.

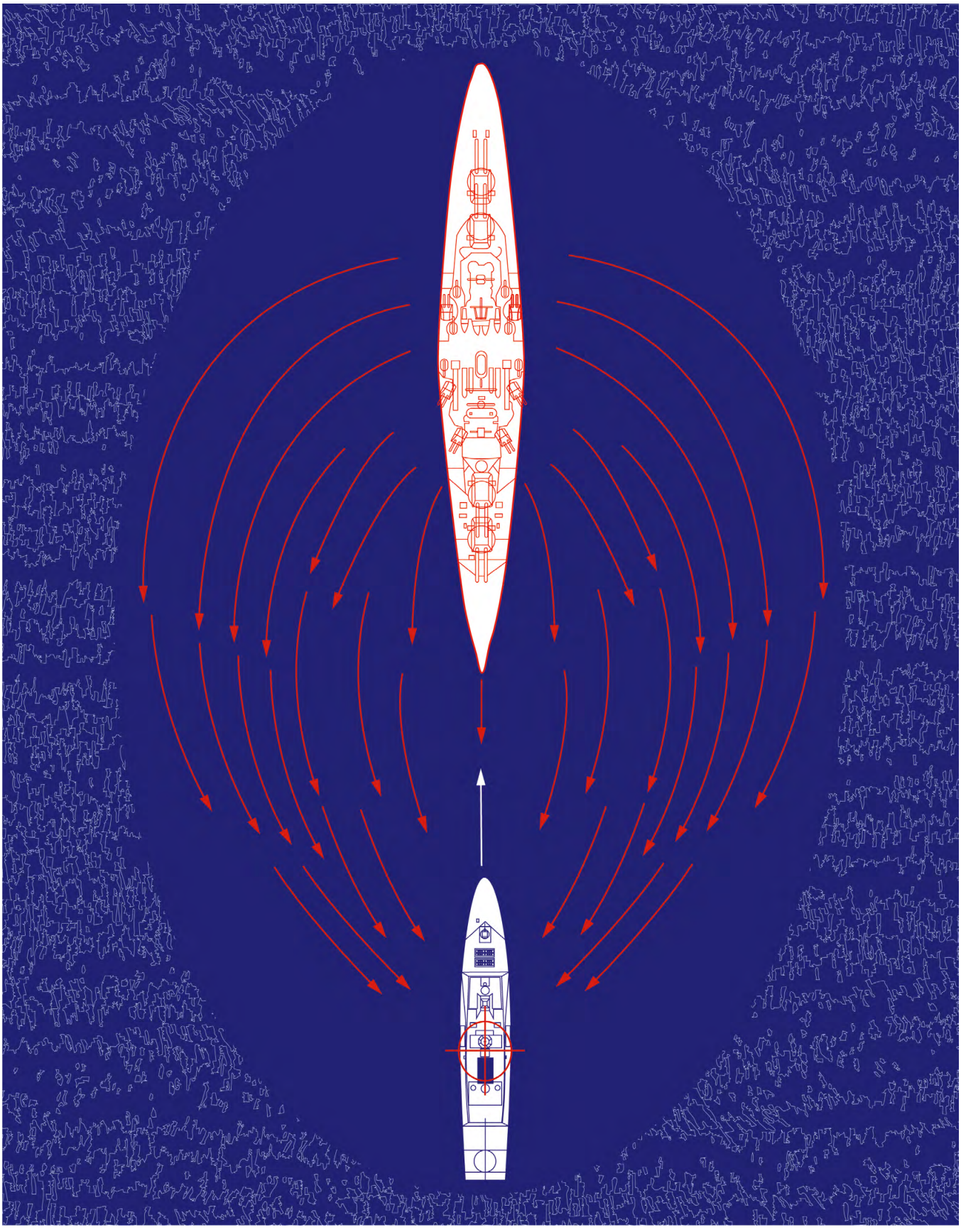
En septembre 2025, le gouvernement a fait le choix d'une gouvernance décentralisée, s'appuyant sur les autorités sectorielles exerçant déjà des missions de surveillance de marché, qui seront coordonnées par la DGE et la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF). L'ANSSI interviendra en appui des autorités de surveillance de marché, pour apporter son expertise sur la cybersécurité des systèmes d'IA. Le Pôle d'expertise de la régulation numérique (PEReN) sera également consulté, sur les sujets de performance et de robustesse des systèmes d'IA. Au cours de l'année 2025, l'Agence a commencé à préfigurer les modalités opérationnelles d'exercice de ces nouvelles missions, en lien avec le PEReN, la DGE et la DGCCRF.

L'ANSSI a également suivi de près les travaux de normalisation du Comité européen de normalisation en électronique et en électrotechnique (CEN/CENELEC) qui visent à définir les exigences applicables en matière de cybersécurité pour les systèmes d'IA à haut risque.

En parallèle, l'Agence s'est impliquée dans le développement de l'INESIA, qui fédère les acteurs français de la sécurité et de l'évaluation de l'IA. Sous le pilotage du SGDSN et de la DGE, l'INESIA structure son activité autour de trois pôles : appui à la régulation de l'IA, risques systémiques et performance, et fiabilité. L'INESIA fédère un écosystème de chercheurs et d'ingénieurs issus de l'ANSSI, de l'Institut national de recherche en sciences et technologies du numérique (Inria), du Laboratoire national de métrologie et d'essais (LNE) et du PEReN, afin de mener à bien les travaux de recherche scientifique qui permettront d'identifier, de mesurer et de faire face aux risques potentiels que les modèles et systèmes d'IA peuvent faire peser sur les intérêts fondamentaux de la Nation. La France rejoint ainsi le réseau international des instituts de sécurité de l'IA (*AI Safety Institutes*). ●

## PANAME, un projet commun pour l'audit de la confidentialité des modèles d'IA

En juin 2025, l'ANSSI, la CNIL, le PEReN et le PEPR Cybersécurité (programme et équipements prioritaires de recherche en cybersécurité financé par France 2030) ont lancé le projet collectif PANAME (*Privacy Auditing of AI Models*). Il vise à développer une bibliothèque logicielle disponible en source ouverte, destinée à unifier les audits de confidentialité des modèles d'IA. La phase de spécification des développements à venir s'est déroulée en 2025. Les travaux se poursuivent, et la bibliothèque devrait être mise à disposition courant 2026. ●



# Engager dès à présent la transition vers la cryptographie post-quantique

La cryptographie post-quantique (communément abrégée en PQC pour *Post Quantum Cryptography*) est un ensemble d'algorithmes de cryptographie, assurant une sécurité contre la menace quantique en plus de leur sécurité classique. La PQC est déployable sur des équipements basés sur les technologies traditionnelles et utilisant les infrastructures de communication existantes.

Pour l'ANSSI, la PQC représente la voie la plus prometteuse pour se prémunir contre la menace quantique. La transition post-quantique durera plus d'une dizaine d'années et impactera l'intégralité de l'écosystème numérique. Sa réussite à l'échelle nationale et européenne est un enjeu majeur de la prochaine décennie.

**↘ Échange avec Samih Souissi, Chef de l'État-Major de la Sous-direction Expertise de l'ANSSI**

***Pourriez-vous expliquer ce qu'est un ordinateur quantique et ses enjeux pour la cybersécurité française ?***
→ Les ordinateurs quantiques sont des calculateurs reposant sur des principes physiques fondamentalement différents des ordinateurs classiques actuels, qui pourraient effectuer certaines tâches beaucoup plus rapidement que ces derniers. Si un ordinateur quantique d'une puissance suffisante venait à être développé, les mécanismes de cryptographie actuellement employés pour protéger notre vie numérique ne seraient plus sûrs. Les impacts seraient potentiellement très lourds : possibilité d'écouter les conversations les plus sensibles ou de pénétrer les systèmes d'information les plus sécurisés.

***Quand ces ordinateurs vont-ils commencer à arriver ? Comment protéger nos infrastructures numériques ?***
→ Compte-tenu de l'investissement mondial sur les technologies de calcul quantique, l'arrivée d'un ordinateur quantique en capacité de compromettre la sécurité des mécanismes cryptographiques est estimée aujourd'hui entre 2035 et 2040. Afin de pouvoir protéger nos infrastructures numériques dans une dizaine d'années, quand cet ordinateur quantique arrivera, il est impératif que les organisations publiques et privées commencent leur transition vers la PQC dès aujourd'hui. L'intégrer aux cycles de renouvellement des systèmes d'information permettra d'en maîtriser les coûts. Le caractère urgent de la situation tient aux délais nécessaires pour développer des produits de confiance intégrant de la cryptographique post-quantique et pour les déployer dans les systèmes d'information. La transition vers la cryptographie post-quantique constitue l'un des enjeux majeurs de la prochaine décennie. ●

## Accompagner la transition vers la cryptographie post-quantique des organisations

L'Agence a pour objectif d'accompagner les organisations dans leur transition vers la PQC.

Afin d'obtenir un état des lieux des pratiques de ses bénéficiaires en matière de PQC, l'ANSSI a mené une étude de marché auprès d'une cinquantaine de ministères et d'entreprises stratégiques. Publiée en mai 2025, l'enquête fait ressortir que de nombreuses entités françaises n'ont pas encore pris la mesure de tous les risques potentiels liés aux ordinateurs quantiques. Mauvaise compréhension des enjeux, manque d'offres et manque de moyens financiers et humains expliquent en partie cette situation. Cette étude vient compléter les deux précédentes, publiées fin 2024, sur les solutions et les prestations de services dans le domaine de la PQC.

L'analyse de ces études a permis à l'Agence de poser une série de recommandations et d'actions.

L'ANSSI conseille aux organisations publiques et privées de démarrer dès à présent un premier travail d'inventaire, afin d'obtenir une bonne visibilité de leurs usages de la cryptographie. Les cas d'usage identifiés comme critiques devront être les premiers à être pris en compte dans une optique de transition vers la cryptographie post-quantique.

L'Agence considère qu'il ne sera pas raisonnable d'acheter des produits qui n'intègrent pas de la PQC après 2030. Les enjeux PQC doivent donc être pris en compte dans le cycle de renouvellement des systèmes d'information, afin que la transition soit anticipée et maîtrisée.

En 2025, l'ANSSI a poursuivi ses efforts de sensibilisation à la PQC par une communication renforcée et un accès aux ressources facilité, ce qui constitue un premier pas vers une meilleure prise de conscience de la nécessité à migrer.

L'Agence a aussi publié cette année de nombreux travaux de recherche sur le sujet (*voir la bibliographie*) et a travaillé sur la mise à jour de ses différents guides et référentiels pour l'intégrer.

Enfin, depuis 2025, le CFSSI propose une formation sur la PQC. Elle présente les grandes lignes de l'état de la menace quantique, aborde principalement le sujet de la transition vers la PQC et explique les problématiques afférentes à cette transition. ●

## Garantir la mise à disposition d'une offre de produits PQC de confiance sur le marché

La transition vers la cryptographie post-quantique ne se fera pas sans la disponibilité de produits de confiance. Aussi, l'ANSSI œuvre dès à présent à la disponibilité d'une offre de solutions PQC de confiance sur le marché, certifiées ou qualifiées par l'Agence, pour les organisations. Au cours de l'année 2025, l'ANSSI, en tant qu'autorité nationale de certification de cybersécurité, a activement travaillé à la bonne prise en compte de la PQC dans les offres de cryptographie.

Le CCN a mis à jour sa doctrine d'agrément cryptographique en mars 2025, et soutient la montée en compétences des centres d'évaluation de la sécurité des technologies de l'information sur le sujet, afin que ceux-ci développent des compétences en matière d'évaluation des mécanismes hybrides (qui combinent les calculs d'un algorithme à clé publique pré-quantique reconnu et d'un algorithme post-quantique supplémentaire), d'évaluation des algorithmes post-quantiques connus, ou encore d'évaluation des attaques par canaux auxiliaires sur certains algorithmes post-quantiques. Cette dernière typologie d'attaque consiste à exploiter les fuites physiques ou temporelles d'un dispositif exécutant un algorithme, plutôt que de casser directement le problème mathématique sous-jacent. L'ANSSI vise la mise en place d'obligations PQC pour l'entrée en qualification de certains produits à partir de 2027.

Le 29 septembre 2025, un premier CESTI a été agréé par l'Agence pour pouvoir officiellement évaluer des solutions intégrant de la PQC. La plupart des CESTI sont actuellement engagés dans le processus d'agrément sur cette nouvelle compétence PQC.

En octobre 2025, le CCN a émis deux premiers certificats pour des solutions comprenant des algorithmes de PQC à base de réseaux euclidiens, qui est une catégorie d'algorithmes de cryptographie post-quantique.

L'ANSSI s'implique également dans le groupe européen de certification en cybersécurité (ECCG), en particulier dans le sous-groupe consacré aux mécanismes cryptographiques. L'objectif est de définir une manière harmonisée d'évaluer l'emploi de la cryptographie dans les produits de sécurité.

En 2025, ce sous-groupe a publié la version 2.0 du document *Agreed Cryptographic Mechanisms*, présentant une liste de mécanismes cryptographiques communément reconnus par les pays membres. Ce document intègre notamment des recommandations sur la PQC. ●

## ↘ Anticiper les grands défis technologiques avec le Conseil scientifique

En 2025, de nombreux projets significatifs ont vu le jour et ont abouti grâce aux travaux du Conseil scientifique de l'ANSSI.

Composé de personnalités scientifiques mais également de représentants étatiques, le Conseil scientifique assure une mission de conseil auprès de l'ANSSI dans le cadre de ses activités de recherche. Organe consultatif de réflexion et de proposition, il accompagne l'ANSSI dans l'anticipation des grands défis technologiques et socio-économiques de la sécurité numérique. En 2025, plusieurs projets de recherche issus des travaux du Conseil scientifique se sont distingués.

Un projet d'étude a été mené par les laboratoires de « cryptographie », d'« architectures matérielles et logicielles » et de « sécurité des technologies sans-fil » afin de comparer du point de vue de la sécurité et de la performance différents mécanismes de chiffrement : le chiffrement complet du disque (*full-disk-encryption*) et le chiffrement basé sur les fichiers (*file-based encryption*). Les experts ont ainsi pu acquérir une meilleure compréhension des mécanismes de chiffrement mis en œuvre par Android et enrichir leur expertise pour être en capacité de formuler des règles ou recommandations de cybersécurité sur les téléphones équipés du système d'exploitation Android.

Par ailleurs, un projet d'étude a été mené en 2025 par le laboratoire « exploration de données et détection » sur les *Graph Foundation Models*, un modèle d'IA capable d'analyser et de généraliser des structures complexes de données sous forme de graphes. Plusieurs applications dans le domaine de la cybersécurité sont envisagées, telles que la détection d'intrusion système ou réseau, ou la CTI (*Cyber Threat Intelligence*).

Autre projet notable, le projet open-source MLA (*Multi-layer archive*) qui a été développé par la sous-direction Opérations pour ses besoins propres (service d'audits automatisés, détection, réponse à incidents, etc.). MLA a été mis à jour en 2025 afin d'intégrer la cryptographie post-quantique, suivant ainsi les préconisations techniques de l'Agence. Le projet est partagé en *open-source* par l'ANSSI sur son GitHub. Cette approche s'inscrit dans une démarche d'ensemble de l'ANSSI visant à partager ses compétences techniques et scientifiques et à apporter de la transparence quant aux outils opérationnels que l'Agence utilise au profit de ses bénéficiaires.

2025 a marqué aussi la fin de mandat du Conseil scientifique avec la remise d'un rapport formulant des propositions et des orientations à l'ANSSI en vue de la mise en place d'un nouveau conseil. ●

### ↘ Accompagner la sécurisation du *cloud*

L'ANSSI a observé en 2025, une augmentation des attaques contre les environnements *cloud*. Ces campagnes d'attaques, menées à des fins lucratives, d'espionnage et de déstabilisation, affectent les fournisseurs de services *cloud* en partie ciblés pour les accès qu'ils peuvent offrir vers leurs clients. Elles ciblent également les environnements de clients de services *cloud*. Les attaquants ont ainsi développé des compétences spécifiques au ciblage des environnements *cloud*.

C'est face à ce constat que l'ANSSI a décidé de publier, en février 2025, un état de la cybermenace pesant sur le secteur du *cloud*, accompagné de recommandations de sécurité à destination des clients de fournisseurs de services *cloud*, ainsi qu'aux fournisseurs de services *cloud* eux-mêmes. Cette publication a été complétée, en octobre 2025, par celle du *Technical Position Paper on Confidential Computing*, qui incite notamment les utilisateurs à rester prudents et à n'adopter cette technologie que lorsque les avantages attendus en matière de sécurité dépassent les coûts de développement, en tenant compte des risques résiduels dans leur modèle de menace.

Pour l'hébergement des données les plus sensibles, il est recommandé de recourir à des offres *cloud* qualifiées SecNumCloud par l'Agence. SecNumCloud est une qualification de sécurité à destination des opérateurs *cloud* permettant d'identifier des offres de confiance.

En 2025, le catalogue des offres SecNumCloud s'est étoffé et diversifié, en réponse aux demandes toujours plus fortes des utilisateurs de recourir à ces offres. L'enrichissement du catalogue illustre également la capacité des offres européennes à appliquer un référentiel exigeant. Une nouvelle marche a été franchie en décembre 2025 avec la qualification d'une offre *cloud* dite « hybride », reposant sur un acteur européen opérant des technologies non européennes.

En avril 2025, Bpifrance a lancé un appel à projets portant sur le renforcement de l'offre de services cloud dans le cadre du plan France 2030. Il vise spécifiquement le domaine du *cloud* de confiance et des services *cloud* pour l'IA. En parallèle, les appels à projets « espace de données mutualisées » et « accompagnement SecNumCloud pour les PME éditeurs de SaaS » se sont poursuivis, mobilisant l'ANSSI sur les différentes phases de ces projets (audition, instruction, suivi). ●

**17**
**offres qualifiées SecNumCloud**

**15**
**offres engagées dans le processus de qualification**

## ↘ Les équipements mobiles, des cibles de choix

En 2025 et dans la continuité des deux années précédentes, l'ANSSI est intervenue de façon croissante sur des cas de compromissions de téléphones mobiles à des fins d'espionnage, appartenant à des individus ayant des fonctions au sein des autorités gouvernementales ou de comités de direction d'entreprises de secteurs stratégiques.

Utilisés quotidiennement par des millions de Français en raison des multiples fonctionnalités qu'ils proposent, les téléphones mobiles sont devenus des cibles de choix pour les attaquants. Les investigations de l'ANSSI et les publications relatives à différents logiciels espions ont démontré un ciblage croissant de téléphones mobiles à des fins d'espionnage, de surveillance mais également lucratives.

Le ciblage de téléphones mobiles peut être effectué par des acteurs étatiques, des cybercriminels, mais également par des entreprises privées, spécialisées dans la lutte informatique offensive privée (LIOP).

Pour y faire face, les États ont un rôle à jouer. C'est pourquoi en novembre 2023, lors du Forum de Paris sur la Paix, la France et le Royaume-Uni ont lancé des consultations pour lutter contre la prolifération et l'usage irresponsable d'outils commerciaux permettant la compromission massive de téléphones. Cette initiative, appelée Processus de Pall Mall depuis son lancement formel à Londres en février 2024, a mené à l'élaboration d'un code de bonnes pratiques à destination des États publié en avril 2025. Pour lutter contre ces menaces, elle encourage à la fois une meilleure coopération des constructeurs pour renforcer la sécurité des équipements mobiles, mais également l'augmentation du partage d'informations sur les menaces observées, tout en recommandant l'établissement de cadres réglementaires relatifs au développement, à l'utilisation et à la vente de telles capacités.

Appliquant ce code de bonnes pratiques, la France, par l'action de l'ANSSI, apporte un soutien aux victimes, mène des actions de sensibilisation et de conseil auprès des populations à risque et incite à l'échange d'informations relatives aux capacités d'intrusion disponibles sur le marché. Elle dispose également d'un cadre réglementaire avec les autorisations prévues aux articles R. 226-3 et R. 226-7 du code pénal, délivrées par le directeur général de l'ANSSI, pour assurer la protection du secret des correspondances et de la vie privée (*voir à ce titre la partie relative au bilan des dispositifs réglementaires de l'Agence*).

En avril 2025, l'ANSSI a publié 10 bonnes pratiques pour l'utilisation des téléphones mobiles afin de sensibiliser largement les Français sur les mesures de sécurité à adopter. En complément, en septembre 2025, l'Agence a publié un document qui met en lumière les notifications envoyées par les constructeurs aux individus ciblés par des attaques menées à l'aide de logiciels espions. Les utilisateurs ayant reçu des notifications de ces constructeurs ont été incités à se manifester auprès de l'ANSSI pour effectuer des investigations et appliquer les mesures de sécurisation nécessaires. Enfin, en novembre 2025, l'Agence a publié un état de la menace sur les équipements mobiles et les recommandations associées pour s'en prémunir. ●

# Bilan des dispositifs réglementaires mis en œuvre par l'ANSSI

**Cette partie présente le bilan des principaux dispositifs réglementaires, hors démarches de qualification et de certification, mis en œuvre par l'ANSSI pour l'année 2025. Inscrits dans le code de la défense et le code des postes et des communications électroniques (CPCE), ces dispositifs permettent à l'Agence de conduire ses missions fixées par le décret n° 2009- 834 du 7 juillet 2009.**

**Ils peuvent être classés selon six finalités :**

- **→ protection des lanceurs d'alerte ;**
- **→ alerte aux victimes ;**
- **→ détection des menaces étatiques et cybercriminelles ;**
- **→ blocage d'une menace affectant la sécurité nationale ;**
- **→ protection de la vie privée et secret des correspondances ;**
- **→ préservation de la sécurité des réseaux 5G et des générations futures.**

# Protection des lanceurs d'alerte

## Ⓐ Toute personne ayant découvert une faille de sécurité ou une vulnérabilité peut la déclarer à l'ANSSI au titre de l'article L.2321-4 du code de la défense.

### PRÉSENTATION DU DISPOSITIF

Ce dispositif légal permet à toute personne de bonne foi qui déclare uniquement à l'ANSSI des vulnérabilités qu'elle aurait pu découvrir sur des systèmes d'information, de voir son identité protégée par l'Agence, en soustrayant les agents de l'ANSSI à leur obligation d'information du Parquet prévue à l'article 40 du code de procédure pénale.

### BILAN 2025

En 2025, l'Agence a été destinataire de 235 signalements au titre de l'article L.2321-4 du code de la défense. La majorité (65 %) de ces signalements ont trait à des vulnérabilités affectant des sites web. Celles-ci peuvent généralement conduire à l'exposition de données, voire à la prise de contrôle de tout ou partie du site. Les expositions de données, qu'elles soient liées à des vulnérabilités ou à des défauts de configuration, représentent 25 % des signalements. Seuls 10 % des signalements reçus par l'ANSSI ont trait à des vulnérabilités affectant des logiciels, généralement des solutions professionnelles. Il est important de souligner que, dans nombre de cas, les déclarants se manifestent en mettant l'entité concernée en copie, levant de fait leur anonymat. ●

## Ⓑ L'ANSSI est chargée, au titre du décret n° 2022-1284 du 3 octobre 2022, pris en application de la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte, de recueillir et de traiter des signalements en matière de sécurité des réseaux et des systèmes d'information émis par les lanceurs d'alerte.

L'ANSSI a été désignée par ce décret comme autorité externe chargée de recueillir et de traiter des signalements émis par les lanceurs d'alerte dans le domaine de la sécurité des réseaux et des systèmes d'information visant, en particulier, celle des opérateurs critiques. Il est ainsi possible pour un lanceur d'alerte de saisir l'Agence en cas de non-respect d'une disposition issue des cadres réglementaires suivants :

- violation d'un dispositif issu de la mise en œuvre des réglementations européennes NIS 1 ou eIDAS, ou des mesures concernant la sécurité des systèmes d'information pour les activités d'importance vitale (SAIV) [5] ;
- non-respect du cadre réglementaire en matière de qualification et de certification de produits ou services ;
- violation d'un contrôle réglementaire [6], comprenant ceux liés à la protection du secret des correspondances ;
- non-respect d'obligations réglementaires imposées aux opérateurs de communications électroniques (OCE) en soutien opérationnel de l'ANSSI [7], comme le défaut de mise à disposition des capacités de détection pour l'identification de victimes ou de caractérisation d'une menace avérée, ou le défaut d'information de l'Agence en cas de détection d'un incident de sécurité sur leurs propres réseaux.

### BILAN 2025

Aucun signalement de nature à donner lieu à une intervention de l'ANSSI, notamment en lien avec un non-respect des dispositifs réglementaires en matière de sécurité des systèmes d'information, n'a été reçu par cette dernière. ●

[5] Pour en savoir plus sur la règlementation NIS et le dispositif SAIV : *https://cyber.gouv.fr/les-directives-nis-nis-2-et-ledispositif-saiv*

[6] Cela concerne notamment le contrôle des moyens de cryptologie (articles 29 à 40 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique), le contrôle R226 (article 226-3 du code pénal – voir la partie E), le régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques de 5e génération (article L34-11 du CPCE – voir la partie E).

[7] Au titre de l'article D.98-5 du code des postes et des communications électroniques (CPCE), de l'article L.33-14, al.2, du CPCE, de l'article L.33-14, al.5, du CPCE et de l'article L.2321-2-1 du code la défense.

# Alerte aux victimes

## Ⓐ L'ANSSI peut alerter les victimes par des campagnes de signalement auprès des opérateurs de communications électroniques au titre de l'article L.33-14 al.5 du code des postes et des communications électroniques.

### PRÉSENTATION DU DISPOSITIF

Ce dispositif permet à l'ANSSI de s'appuyer sur les OCE ayant le statut d'opérateur d'importance vitale (OIV), pour transmettre des messages de signalement de vulnérabilités ou de compromissions auprès d'abonnés concernés.

### BILAN 2025

En 2025, trois campagnes de signalement de vulnérabilités représentant 33 085 adresses IP ont été menées auprès des abonnés des opérateurs. 25 419 d'entre elles ont pu être identifiées. L'ensemble des OCE concernés a participé aux trois campagnes. Le site cybermalveillance.gouv.fr héberge les pages d'alerte vulnérabilité vers lesquelles les opérateurs redirigent leurs clients dans le cadre de ces campagnes, permettant de mesurer le suivi de ces dernières. Ainsi, 2 004 consultations de ces pages ont été effectuées directement en lien avec ces campagnes. ●

## Ⓑ L'ANSSI peut demander des éléments d'identification des victimes auprès des opérateurs de communications électroniques au titre de l'article L.2321-3 al.1 du code de la défense.

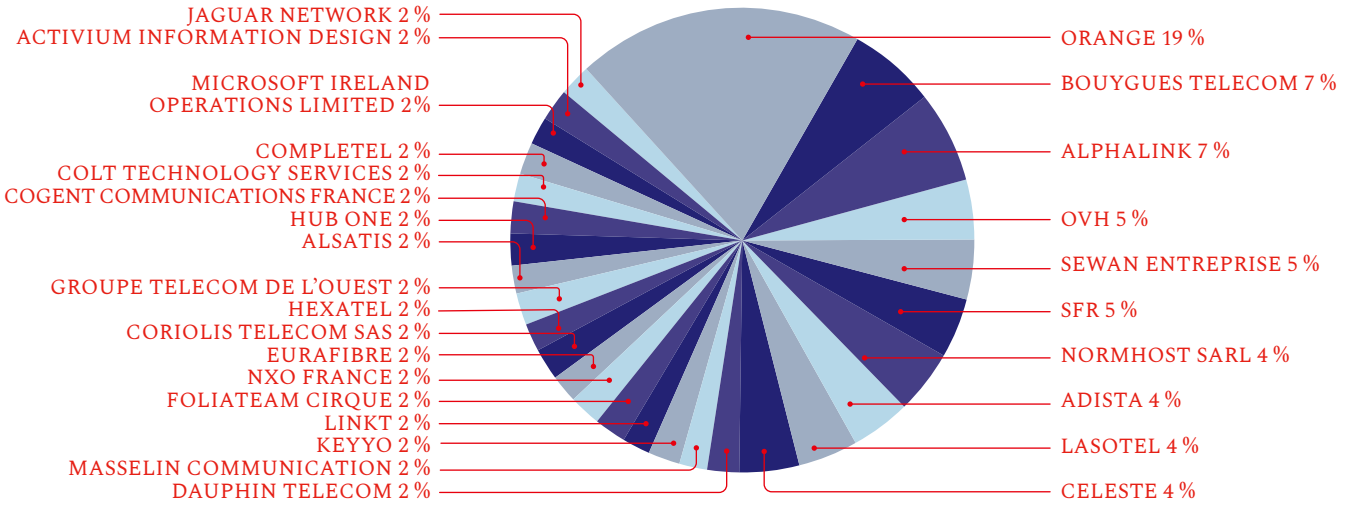
### PRÉSENTATION DU DISPOSITIF

Cet article précise dans quels cas l'ANSSI peut demander des informations aux OCE. L'alinéa premier prévoit que, pour les besoins de la sécurité des systèmes d'information d'un OIV, d'un opérateur de service essentiel (OSE) ou d'une autorité publique, l'Agence peut demander à l'OCE l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués. Le but est de les alerter sur la vulnérabilité ou l'attaque de leur système d'information. Ces identifications répondent au besoin de sécurisation des opérateurs réglementés.

### BILAN 2025

En 2025, 47 demandes d'identification pour un total de 718 adresses IP ont été effectuées par l'ANSSI auprès de 28 opérateurs de communications électroniques. Orange, Bouygues et Alphalink concentrent près d'un tiers des demandes (31,9 %). L'article L.2321-3 al.1 du code de la défense est indispensable aux missions d'alerte de l'Agence, en complément des autres outils mis à disposition. En effet, l'ANSSI recherche des potentielles victimes dans l'ensemble des bases à sa disposition avant d'utiliser ce dispositif et celles-ci sont, au fil des ans, plus nombreuses et plus précises. ●

**RÉPARTITION DES DEMANDES D'IDENTIFICATION DES VICTIMES AU TITRE DE L'ARTICLE L.2321-3 AL.1 DU CODE DE LA DÉFENSE PAR OPÉRATEUR DE COMMUNICATIONS ÉLECTRONIQUES**



# Alerte aux victimes

**Ⓒ L'article L.2321-4-1 du code de la défense nationale oblige les éditeurs à notifier à l'ANSSI les vulnérabilités significatives affectant leurs produits distribués en France.**

## PRÉSENTATION DU DISPOSITIF

L'article L.2321-4-1 du code de la défense nationale a été créé par la loi de programmation militaire (LPM) 2024-2030. Il crée une nouvelle obligation à la charge des éditeurs : la déclaration des vulnérabilités significatives à l'ANSSI et à leurs utilisateurs.

Son objectif est d'améliorer la prise en compte des vulnérabilités jusqu'à leur correction, ainsi que la communication auprès des utilisateurs afin de mieux protéger leurs systèmes d'information. Cette disposition prévoit la coordination du traitement de la vulnérabilité significative par l'Agence avec l'ensemble des parties intéressées. Lorsque l'éditeur manque à ses obligations de communication auprès des utilisateurs, l'ANSSI a la faculté de l'enjoindre à communiquer ainsi que de communiquer publiquement ou non sur la vulnérabilité, et de publier l'injonction en cas de manquements persistants de l'éditeur.

L'article L.2321-4-1 fait l'objet d'un amendement pour mise en conformité vis-à-vis du Règlement européen sur la résilience cyber, portant également sur les responsabilités des éditeurs concernant les vulnérabilités, dans le cadre du projet de loi portant diverses dispositions d'adaptation au droit de l'UE en matière économique, financière, environnementale, énergétique, d'information, de transport, de santé, d'agriculture et de pêche, en cours de discussion au Parlement.

## BILAN 2025

En 2025, l'ANSSI a traité 15 vulnérabilités significatives entrant dans le champ d'application de l'article L.2321-4-1 du code de la défense nationale. Toutefois, les déclarations reçues ont été dans leur majorité réalisées après la correction des vulnérabilités et l'avertissement des clients. Les déclarations réalisées avant la correction ont permis d'établir un dialogue satisfaisant avec les éditeurs concernés. ●

# Détection des menaces étatiques et cybercriminelles

## Ⓐ Les opérateurs de communications électroniques doivent recourir à des dispositifs de détection et exploiter les marqueurs techniques fournis par l'ANSSI au titre de l'article L.33-14 al.1 et 2 du code des postes et des communications électroniques (CPCE) complété par l'article L.2321-3 al.2 du code de la défense.

### PRÉSENTATION DU DISPOSITIF

Les opérateurs de communications électroniques, par leur rôle d'interconnexion entre les différents réseaux informatiques de leurs clients, occupent une position clé pour permettre la détection des attaques informatiques.

L'article L.33-14 du CPCE prévoit dans son deuxième alinéa que l'ANSSI puisse fournir des marqueurs que les OCE mettent en exploitation dans leurs systèmes de détection. Ces marqueurs permettent de déclencher des alertes qui conduisent *in fine* à identifier et alerter des victimes.

### BILAN 2025

Aujourd'hui, les opérateurs parviennent à mettre en œuvre les marqueurs de l'Agence en utilisant des éléments de leur infrastructure qui n'ont pas été conçus pour répondre à ce besoin. L'ANSSI a réalisé une campagne en 2025 sur la base de ces capacités. L'Agence s'appuie actuellement sur le Commissariat aux communications électroniques de défense (CCED) pour assurer le déploiement de capacités permettant de mieux répondre aux besoins des opérateurs afin de remplir la mission confiée par la loi. ●

## Ⓑ L'ANSSI peut mettre en place un dispositif de détection sur des équipements contrôlés par des attaquants chez des opérateurs de communications électroniques ou des hébergeurs, au titre de l'article L.2321-2-1 du code de la défense.

### PRÉSENTATION DU DISPOSITIF

Issu de la LPM 2019-2025 et renforcé par la LPM 2024- 2030, l'article L.2321-2-1 du code de la défense autorise l'ANSSI à mettre en place des dispositifs permettant le recueil de données chez des opérateurs de communications électroniques ou des hébergeurs afin d'observer un équipement contrôlé par des attaquants.

Ce dispositif, strictement contrôlé par l'Autorité de Régulation des Communications Électroniques, des Postes et de la distribution de la Presse (ARCEP), est réservé aux menaces portant atteinte à la défense et à la sécurité nationale ou aux opérateurs critiques (OIV, OSE, autorités publiques). Il a permis l'identification de victimes de menaces informatiques en France et à l'étranger.

### BILAN 2025

En 2025, 7 opérations ont été lancées auprès d'hébergeurs, dont une a été prorogée. Une opération initiée en 2024 a été prorogée à plusieurs reprises au-delà de la durée initiale de trois mois afin de maintenir un suivi dans le temps long d'une menace affectant la sécurité nationale. ●

# Détection des menaces étatiques et cybercriminelles

## Ⓒ Communication à l'ANSSI de données techniques de cache de serveurs DNS : article L.2321-3-1 code de la défense.

### PRÉSENTATION DU DISPOSITIF

Cette disposition impose aux fournisseurs de système de résolution de noms de domaine de transmettre régulièrement à l'ANSSI les données de cache enregistrées par leur système de résolution de noms de domaine (*Domaine Name System* ou DNS). Ces données non identifiantes permettent d'associer les noms de domaine et leurs adresses IP, et sont exploitées à des fins d'analyse et de caractérisation des menaces.

La disposition vise à améliorer la connaissance des acteurs offensifs susceptibles de porter atteinte à la sécurité nationale qui utilisent des noms de domaine pour mener leurs attaques informatiques, en permettant notamment d'identifier d'autres éléments de leurs infrastructures d'attaque ou de préciser la chronologie des attaques. Les données dites de « cache DNS » sont fondamentales à l'analyse de la menace et peuvent également être obtenues à partir de sources commerciales, pour certaines.

### BILAN 2025

Les échanges engagés en 2024 se sont poursuivis auprès des différents opérateurs de communications électroniques pour permettre la mise en œuvre de cette mesure. La mobilisation de l'ensemble des acteurs est notable et l'ANSSI dispose de différentes options pour mettre en œuvre cette mesure. Un premier opérateur est en mesure de fournir ses données à l'Agence et les autres devraient être en mesure de le faire au cours de l'année 2026. ●

# Blocage d'une menace affectant la sécurité nationale

## PRÉSENTATION DU DISPOSITIF

L'article L.2321-2-3 du code de la défense dote l'ANSSI du pouvoir de demander le filtrage de noms de domaine utilisés par des attaquants. En cas de menace susceptible de porter atteinte à la sécurité nationale, et sous le strict contrôle de l'ARCEP, l'Agence peut prescrire des mesures graduelles de filtrage de noms de domaine aux fournisseurs de résolveurs DNS, aux bureaux d'enregistrement et à l'office d'enregistrement.

Parmi les dispositions, l'ANSSI peut demander le blocage ou la suspension du nom de domaine, permettant ainsi de neutraliser son utilisation à des fins malveillantes. Toutefois, pour des menaces avancées, cette action ne permet pas d'entraver durablement les actions de l'attaquant. Il est ainsi prévu que l'Agence puisse demander la redirection ou le transfert de noms de domaine, afin d'observer les requêtes à destination de ce dernier, et donc d'identifier des victimes. Une fois alertées par l'ANSSI, ces victimes sont en capacité de mettre en place des mesures d'endiguement puis de remédiation durable de l'attaque.

## BILAN 2025

L'Agence dispose de la capacité de blocage et redirection auprès des principaux OCE. Une seule menace détectée a nécessité l'utilisation de ce dispositif au cours de l'année 2025. ●

# Protection de la vie privée et du secret des correspondances

En France, la commercialisation et l'exploitation de dispositifs ou d'appareils techniques pouvant porter atteinte à la vie privée et au secret des correspondances sont rigoureusement contrôlées.

L'ANSSI est chargée de ce contrôle qui s'exerce au travers d'un régime d'autorisation administrative préalable instauré par les articles 226-3 et 226-7 du code pénal.

## PRÉSENTATION DU DISPOSITIF

Afin de protéger la vie privée et le secret des correspondances, le code pénal prévoit aux articles 226-3 et 226-7 l'obtention d'une autorisation préalable à la fabrication, l'importation, l'acquisition, la détention, l'exposition, l'offre, la location ou la vente de certains équipements.

Ce régime concerne aussi bien le fabricant ou le revendeur, que l'exploitant du dispositif. On distingue ainsi l'autorisation requise pour « la fabrication, l'importation, l'exposition, l'offre, la location ou la vente », prévue à l'article 226-3 du code pénal, de celle requise pour « l'acquisition ou la détention », prévue à l'article 226-7 du même code.

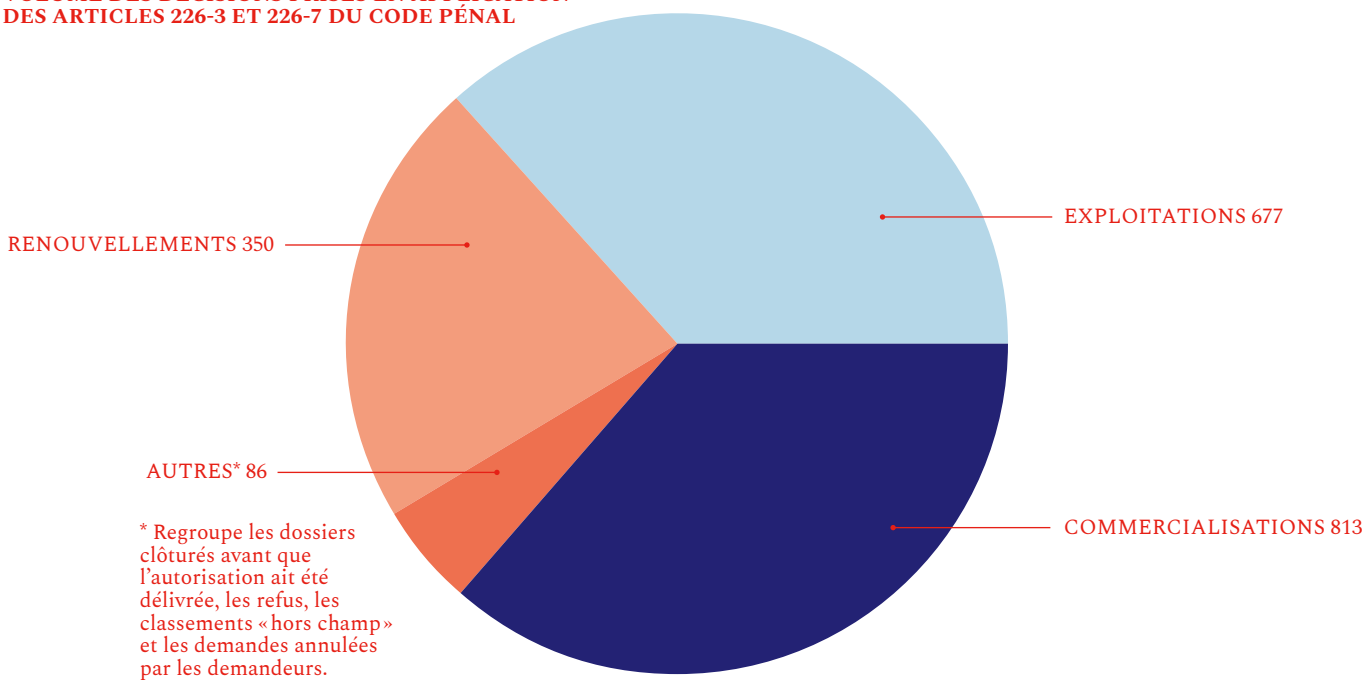
La demande d'autorisation est instruite par les services de l'Agence, qui s'assurent en particulier que le dispositif correspond à un usage légitime prévu par le droit français, qu'il est adéquatement sécurisé et n'est pas détournable de son usage légitime. Elle est ensuite étudiée par une commission consultative présidée par le directeur général de l'ANSSI et composée de représentants des administrations concernées (ministères de la Justice, de l'Intérieur, des Armées, des Douanes, de l'Industrie, des Télécommunications, Agence nationale des fréquences, Commission nationale de contrôle des techniques de renseignement).

Outre le délai, qui selon les cas varie d'un à six ans, l'autorisation peut fixer le nombre d'appareils concernés et subordonner leur utilisation à des conditions destinées à en éviter tout usage abusif.

## BILAN 2025

L'ANSSI a rendu 1926 décisions en 2025, dont 72 décisions de refus. ●

**VOLUME DES DÉCISIONS PRISES EN APPLICATION DES ARTICLES 226-3 ET 226-7 DU CODE PÉNAL**




* Regroupe les dossiers clôturés avant que l'autorisation ait été délivrée, les refus, les classements « hors champ » et les demandes annulées par les demandeurs.

# Préservation de la sécurité des réseaux 5G et des générations futures

Depuis 2019, l'ANSSI contrôle les équipements utilisés dans le cadre du déploiement des réseaux 5G afin de garantir leur sécurité. Ce contrôle est exercé au titre de l'article L.34-11 du CPCE.

## PRÉSENTATION DU DISPOSITIF

L'article L.34-11 du CPCE soumet à autorisation du Premier ministre, dans le but de préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des matériels ou logiciels permettant de connecter les terminaux des utilisateurs finaux au réseau 5G et qui présentent un risque pour la permanence, l'intégrité, la sécurité, la disponibilité du réseau, ou pour la confidentialité des messages [8].

Ce dispositif, dont la mise en œuvre relève du SGDSN, ne concerne que les réseaux de cinquième génération dits « 5G », et s'appliquera également aux générations suivantes.

Il vise à tenir compte des risques que font peser les nouvelles capacités des infrastructures mobiles sur la défense et la sécurité nationale. Il constitue à cet égard une réponse aux évolutions fondamentales inhérentes au déploiement des technologies 5G, qui ne pouvaient pas être prises en compte de manière adéquate par le régime « R. 226 » présenté dans la partie précédente :

- l'apparition de nombreux usages nouveaux, comme la télémédecine, les transports ou l'industrie connectée, ainsi que la convergence au sein des réseaux 5G publics de cas d'usages portés jusqu'alors par des réseaux spécifiques et isolés. Du fait de ces usages, la compromission de l'intégrité ou de la disponibilité des réseaux 5G pourrait avoir des conséquences très graves tant sur la sécurité des biens et des personnes que sur la continuité de l'action de l'État ;
- l'évolution des infrastructures de réseaux radioélectriques mobiles vers des applications principalement logicielles, portées par des technologies informatiques génériques, en lieu et place des technologies hautement spécialisées mises en œuvre dans les générations précédentes. Cette évolution offre aux opérateurs qui déploient et exploitent de telles infrastructures une grande liberté de configuration mais les expose également à toutes les menaces et vulnérabilités liées à ces technologies génériques ;
- le rôle central que les réseaux 5G sont amenés à jouer pour la majorité des usages numériques confère à ces derniers une très haute importance stratégique qui pourrait les exposer à des tentatives d'ingérence par des États tiers, y compris par le biais des pressions que de tels États pourraient exercer à l'égard des opérateurs ou de leurs fournisseurs et prestataires.

Les types d'appareils soumis à autorisation sont définis par arrêté. Il s'agit, d'une part, des stations de base, soit les antennes déployées à travers l'ensemble du territoire qui assurent la connectivité des équipements terminaux des usagers et, d'autre part, d'un ensemble de fonctions jugées critiques au sein des cœurs de réseau, infrastructures centrales des réseaux mobiles.

## BILAN 2025

### Les décisions relatives aux antennes 5G

Pour l'année 2025, 160 décisions ont été rendues, dont 7 décisions de refus. Il convient de préciser que les demandes d'autorisation sont généralement déposées pour des groupes d'antennes si bien qu'une décision peut concerner plusieurs dizaines de stations de base. Par ailleurs, comme chaque mise à jour majeure doit faire l'objet d'une nouvelle autorisation, le nombre de décisions rendues ne reflète pas véritablement l'évolution du parc antennaire : une même antenne peut faire l'objet d'autorisations successives à l'occasion des évolutions de versions logicielles.

Dans les faits, 75 % des décisions prises après 2020 concernent des demandes de renouvellement d'autorisations dans le cadre de mise à jour logicielle.

### Les décisions relatives aux cœurs de réseau 5G

Jusqu'en juin 2023, les opérateurs ont déposé des demandes d'autorisation uniquement pour des stations de base (antennes). En effet, dans le premier temps de son déploiement en France, la 5G a été mise en œuvre dans une configuration dite *Non Standalone* (ou « NSA »), laquelle repose sur des cœurs de réseau de quatrième génération (4G), qui n'entrent pas dans le champ de l'article L.34-11 du CPCE.

S'agissant de la 5G dite *Standalone* (ou « SA »), les premières demandes portant sur la partie cœur de réseau ont été déposées à partir de juillet 2023. Au cours de l'année passée, 47 autorisations ont été délivrées pour des équipements des cœurs de réseau de cinquième génération. ●

[8] Cette mesure a été introduite par la loi n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles.

# Bibliographie

## GUIDES DE BONNES PRATIQUES

### → LES ESSENTIELS

*Bases de données relationnelles*, version 1.0.
En savoir plus

*Se protéger des fuites de données*, version 1.0.
En savoir plus

*Données et traitements sensibles*, version 1.0.
En savoir plus

*Hygiène numérique des téléphones mobiles*, version 1.0.
En savoir plus

*Sélection d'un logiciel libre*, version 1.0.
En savoir plus

*Modèle Zero Trust*, version 1.0.
En savoir plus

*Infrastructure de gestion de clés (IGC)*, version 1.0.
En savoir plus

*Architecture sécurisée de SI*, version 1.0.
En savoir plus

*Mise en œuvre sécurisée d'un serveur Windows*, version 1.0.
En savoir plus

### → LES BACK TO BASICS (version anglaise des Essentiels)

*Relational database*, version 1.0.
En savoir plus

*Data leak prevention*, version 1.0.
En savoir plus

*Sensitive data and processing*, version 1.0.
En savoir plus

*Digital hygiene for mobile phones*, version 1.0.
En savoir plus

*How to select an open-source software*, version 1.0.
En savoir plus

*Zero Trust Model*, version 1.0.
En savoir plus

*Public key infrastructure (PKI)*, version 1.0.
En savoir plus

*Information system security infrastructure*, version 1.0.
En savoir plus

*Start-up security for Windows servers*, version 1.0.
En savoir plus

### → LES FONDAMENTAUX

*Automatisation de la gestion des certificats avec ACME*, version 1.0.
En savoir plus

*Zero Trust*, version 1.0.
En savoir plus

### → LES GUIDES TECHNIQUES

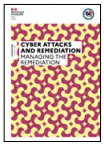
*La cybersécurité des systèmes industriels – Méthode de classification*, version 2.0.
En savoir plus

*La cybersécurité des systèmes industriels – Mesures détaillées*, version 2.0.
En savoir plus

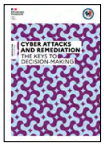
*La supervision de sécurité : les clés de décision*, version 1.0.
En savoir plus

*La supervision de sécurité : piloter un projet de supervision*, version 1.0.
En savoir plus

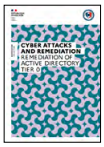
*L'homologation de sécurité des systèmes d'information*, version 1.0.
En savoir plus



*Cyber attacks and remediation: Managing the remediation*, version 1.0.
En savoir plus



*Cyber attacks and remediation: The keys to decision-making*, version 1.0.
En savoir plus



*Cyber attacks and remediation: Remediation of active directory tier 0*, version 1.0.
En savoir plus

### → LES RETEX D'EXERCICES DE CRISE

*Retour d'expérience sur l'exercice de crise cyber du Sommet de l'IA*. 11 février 2025.
En savoir plus

*Retour d'expérience (RETEX) de l'exercice REMPAR25*. 18 septembre 2025.
En savoir plus

## PUBLICATIONS SCIENTIFIQUES

*Silithium: signature hybride made in ANSSI Compact, Efficient and Non-Separable Hybrid Signatures* (J. Devevey, M. Guerreau, M. Roméas)

*Chiffrement actualisable fondé sur les isogénies* (A. Leroux, M. Roméas)

*Établissement authentifié de clé compacti via double-KEM* (H. Beguinet, C. Chevalier, G. Lebrun, T. Legavre, T. Ricosset, M. Roméas, E. Sageloli) (e2025/1755)

*Breaking Hufu with 0 Leakage* (J. Devevey, M. Guerreau, T. Legavre, A. Martinelli, T. Ricosset) (e2025/548 + Cascade 2025)

*SUCRE* (masquage ML-DSA, S. Belaïd, R. Benadjila, J. Devevey, M. Guerreau, T. Legavre, A. Martinelli, T. Ricosset, M. Rivain et M. Rossi)

*Analyse du cryptosystème McEliece* (H. Randriam, N. Marteau, P. Perrier, M. Boutros)

### → THÈSES DE DOCTORAT

*Vers une méthode d'analyse de la sécurité des protocoles de communication sans-fil*, T. Claverie, thèse de doctorat, INSA de Rennes, 2025.
En savoir plus

*A tale of trees, or security and efficiency of secure group messaging protocols*, G. Lebrun, thèse de doctorat, École Normale Supérieure, 2025.

### → ARTICLES SCIENTIFIQUES PRÉSENTÉS EN CONFÉRENCE

*Approche SSI pour l'Internet des objets industriels*, conférence C&ESAR23.
En savoir plus

*Overlapping data in network protocols: bridging OS and NIDS reassembly gap*, L. Aubard, [**J. Mazel**], G. Guette, [**P. Chifflier**], DIMVA 2025.
En savoir plus

*Overlapping IPv4, IPv6, and TCP data: exploring errors, test case context, and multiple overlaps inside network stacks and NIDSes with PYROLYSE*, L. Aubard, [**J. Mazel**], G. Guette, [**P. Chifflier**], RAID 2025.
En savoir plus

*Improved Resultant Attack against Arithmetization-Oriented Primitives*, [**A. Bariant**], A. Bœuf, P. Briaud, M. Hostettler, M. Øygarden et H. Raddum, CRYPTO 2025.
En savoir plus

*Corrigendum to Fast AES-Based Universal Hash Functions and MACs*, [**A. Bariant**], J. Baudrin, G. Leurent, C. Pernot, L. Perrin et T. Peyrin, IACR Transactions on Symmetric Cryptology (ToSC) 2025, volume 1 pp 623-628.
En savoir plus

*Optimal Dimensionality Reduction using Conditional Variational AutoEncoder*, S. Boussam, M. Carbone, [**B. Gérard**], [**G. Renault**], G. Zaid, IACR Transactions on Cryptographic Hardware and Embedded Systems 2025(3): 164-211 (2025).
En savoir plus

*The Art of Bonsai: How Well-Shaped Trees Improve the Communication Cost of MLS*, C. Chevalier, [**G. Lebrun**], [**A. Martinelli**] et [**J. Plût**], EuroS&P 2025.
En savoir plus

*Leaking-cascades : an optimized construction for KEM hybridization*, C. Chevalier, [**G. Lebrun**], [**A. Martinelli**], ACNS 2025.
En savoir plus

*To Be, or Not to Be a Nonce: Formal Analysis of Random Nonce Misuses in Cryptographic Protocols*, [**T. Claverie**], G.Avoine, S.Delaune, 38th IEEE Computer Security Foundations Symposium (CSF 2025), volume 1 pp 623-628.
En savoir plus

*Dealing with TEMPEST threat in its entirety – beyond video emanations in electric field*, [**E. Cottais**], 2025 International Symposium on EMC Europe 2025.
En savoir plus

*Breaking HUFU with 0 Leakage: A Side-Channel Analysis*, [**J. Devevev**], M. Guerreau, T. Legavre, [**A. Martinelli**] et T. Ricosset, CASCADE 2025.
En savoir plus

*A Formal Security Analysis of OPC-UA*, [**V. Diemunsch**], Lucca Hirsch et Steve Kremer, USENIX 2025.
En savoir plus

*On the Success Rate of Simple Side-Channel Attacks Against Masking with Unlimited Attack Traces*, A. Hiltenbrand, J. Eynard, [**R. Poussier**], CASCADE 2025: 343-366.
En savoir plus

*Identification d'images de micrologiciels*, [**A. Iooss**], SSTIC 2025.
En savoir plus

*Electromagnetic Security: a practical approach*, [**J. Lopes Esteves**], [**E. Cottais**], 12th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2025).
En savoir plus

*Intentional Electromagnetic Interference and wireless communication systems: impact, detection and localization of attack sources*, [**J. Lopes Esteves**], V.Deniau, C.Gransart, 2025 International Symposium on EMC Europe 2025.
En savoir plus

*A formal tale of two worlds, a story of WireGuard hybridization*, D. Mahmoud, P. Lafourcade, [**S. Ruhault**] et [**A. Rahman Taleb**], USENIX 2025.
En savoir plus

*Striking Back At Cobalt: Using Network Traffic Metadata To Detect Cobalt Strike Masquerading Command and Control Channels*, [**C. Parssegny**], [**J. Mazel**], O. Levillain, [**P. Chifflier**], ARES 2025.
En savoir plus

*Investigation aux frontières du système : cas d'un reset factory aléatoire*, [**P-M. Ricordel**], [**M. Smaha**], SSTIC 2025.
En savoir plus

*Harnessing IMS implementation(s): a two-sided [s]wor[l]d*, [**G. Teissier**], [**T. Claverie**], Troopers TelcoSecDay 2025.
En savoir plus

*Towards package opening detection at power-up by monitoring thermal dissipation*, [**J. Toulemont**], G. Chancel, F. Mailly, P. Maurine et P. Nouet, CASCADE 2025.
En savoir plus

*300 secondes chrono : prise de contrôle d'un infodivertissement automobile à distance*, [**P. Trébuchet**] et [**G. Bouffard**], SSTIC' 25.
En savoir plus

### → CONTRIBUTIONS À DES OUVRAGES SCIENTIFIQUES

*Real Do Not Trust Power Management: A Survey on Internal Energy-based Attacks Circumventing Trusted Execution Environments Security Properties*, G. Le Gonidec, G. Bouffard, J. -C. Prévotet, et M. Méndez, ACM Transactions on Embedded Computing Systems (2025).
En savoir plus

*Protected AES Implementations*, F. Rondepierre, Chapter 8, pp. 177-199, Embedded Cryptography – Book 2 (eds E. Prouff, G. Renault, M. Rivain and C. O'Flynn), Encyclopedia Sciences ISTE-WILEY

[**P.Nom**] *Personnes rattachées à l'ANSSI au moment de la soumission ou de la publication de l'article scientifique.*

## PUBLICATIONS *OPEN SOURCE*

FaQ sur la cryptographie post-quantique (PQC).
En savoir plus

**Chipsec-check** : logiciel pour générer une clé USB *bootable* incluant notamment l'outil chipsec et permettant de tester la conformité des exigences de sécurité matérielle et logicielle attendues dans les configurations matérielles et UEFI des portables expertisés dans le cadre du marchés ODICE et ODICE2.
En savoir plus

**Decode** : outil de détection de binaires anormaux dans le cadre d'une investigation numérique sur une machine Windows.
En savoir plus

**IPECC** : une implémentation matérielle pour calculer une multiplication scalaire [k] P sur des courbes elliptiques définies sous la forme short Weierstrass sur des corps finis de caractéristique p>3.
En savoir plus

**Lidi** : une diode logicielle développée en Rust.
En savoir plus

**PYROLYSE** : outil d'extraction et de test des politiques de recouvrement dans les protocoles réseau au sein des piles réseau et IDS.
En savoir plus

**Tamarin parser** : outil permettant la mutation automatisée de l'arbre syntaxique abstrait des modèles de protocoles définis avec Tamarin Prover, permettant d'analyser des protocoles sous diverses conditions.
Code source Github

## CONTRIBUTIONS À DES PROJETS *OPEN SOURCE* TIERS

**Chipsec** : un *framework* pour analyser la sécurité des plateformes PC, y compris le matériel, le *firmware* système (BIOS/UEFI) et les composants de la plateforme ; un agent assure la maintenance pour l'architecture AMD et a contribué à l'ajout de support pour la construction d'image USB.
Code source Github

**Decret** : un outil qui reproduit un environnement Debian vulnérable pour un numéro de CVE donné.
Code source Github

**Linux Hardened** : projet visant à renforcer la sécurité du noyau Linux en appliquant un ensemble minimal de correctifs et de configurations qui complètent le Kernel Self Protection Project (KSPP) en amont. L'objectif principal est de fournir des fonctionnalités de sécurité supplémentaires qui ne sont pas couvertes par SELinux et Yama, en se concentrant principalement sur les architectures multiarch arm64 et x86_64.
Code source Github

**Linux PAM** (Pluggable Authentication Modules) : une suite de librairies et de modules qui permettent à un administrateur de système Linux de configurer diverses méthodes d'authentification pour ses utilisateurs (mots de passe locaux, LDAP, Yubikeys, cartes à puce, certificats…).
Code source Github

**Noyau Linux** : des corrections de vulnérabilités de type corruption de la mémoire et confusion de types ont été réalisées ainsi que des contributions à plusieurs Linux Security Modules (LSM) tels que Landlock, Kernel lockdown ou AppArmor.
Code source Github

**Scapy** : un outil de manipulation de paquets réseaux écrit en Python.
Code source Github

**Sentry** : un micro-noyau qui présente des propriétés de sécurité pertinentes telles que le cloisonnement des applications utilisateurs, vérifié par des méthodes formelles (Frama-C) pour l'absence d'erreur d'exécution et le durcissement de la mémoire.
Code source Github

**Suricata** : un logiciel d'analyse réseau et de détection des menaces.
Code source Github

**Systemd** : un gestionnaire de systèmes et de services pour les systèmes d'exploitation Linux auquel a été apporté des corrections du comportement de l'*enrollement* des clés de démarrage sécurisé afin de respecter la spécification UEFI.
Code source Github

**Zeek** : un *framework* pour l'analyse de trafic réseau et la surveillance de la sécurité.
Code source Github

## RAPPORTS SUR LES MENACES ET INCIDENTS

*Panorama de la cybermenace 2024*. 11 mars 2025.
En savoir plus

*Cyber Threat Overview 2024*. 11 mars 2025.
En savoir plus

*Secteur du cloud - État de la menace informatique*. 20 février 2025.
En savoir plus

*Collectivités territoriales – Synthèse de la menace*. 24 février 2025.
En savoir plus

*Transports urbains – État de la menace informatique*. 13 avril 2025.
En savoir plus

*Ciblage et compromission d'entités françaises au moyen du mode opératoire d'attaque APT28*, 29 avril 2025.
En savoir plus

*Targeting and compromise of French entities using the APT28 intrusion set*. 29 avril 2025.
En savoir plus

*Opération ENDGAME 2025* de 23 mai 2025.
En savoir plus

*Opération ENDGAME* de novembre 2025. 13 novembre 2025.
En savoir plus

*Houken seeking a path by living on the edge with zero-days*. 4 juillet 2025.
En savoir plus

*Téléphones mobiles : État de la menace depuis 2015*. 26 novembre 2025.
En savoir plus

*Mobile phones : Threat landscape since 2015*. 26 novembre 2025.
En savoir plus

*Campagne de notifications de menace envoyée par Apple*. 8 décembre 2025.
En savoir plus

## PUBLICATIONS CONJOINTES

*Technical position paper on Confidential Computing.*
En savoir plus

*A shared vision of software bill of materials (SBOM) for cybersecurity.*
En savoir plus

*Remote Identity Proofing for EUDI Wallet Onboarding: Strengthening Assurance Against Evolving Threats.*
En savoir plus

*Russian GRU Targeting Western Logistics Entities and Technology Companies.*
En savoir plus

*Joint Statement by ANSSI and BSI on Cloud Sovereignty Criteria.*
En savoir plus

*A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity.*
En savoir plus

*Design Principles for LLM-based Systems with Zero Trust.*
En savoir plus

*A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography.*
En savoir plus

*Développer la confiance dans l'IA par une approche par les risques cyber.*
En savoir plus

*Building trust in AI through a cyber risk-based approach.*
En savoir plus

## ÉTUDES DE MARCHÉ

*État de la prise en compte de la cryptographie post-quantique par les bénéficiaires de l'ANSSI en 2023.*
En savoir plus

*L'IA au service de la détection et de la réponse à incident.*
En savoir plus

## RÉFÉRENTIELS

*Référentiel d'exigences applicables aux prestataires de réponse aux incidents de sécurité (PRIS), version 3.2 du 28 octobre 2025.*
En savoir plus

## FICHES TECHNIQUES

*Profil de protection – Video IP, Camera.*
En savoir plus

*Profil de protection – Video IP, VMS.*
En savoir plus

Version 1.0 – Mai 2026
Dépôt légal : mai 2026
ISSN 2804-5920 (en ligne)


**Agence nationale
de la sécurité des
systèmes d'information**
ANSSI
51 boulevard
de la Tour-Maubourg
75700 PARIS 07 SP
*www.cyber.gouv.fr*

**Design graphique
& illustrations :**
Cercle Studio