



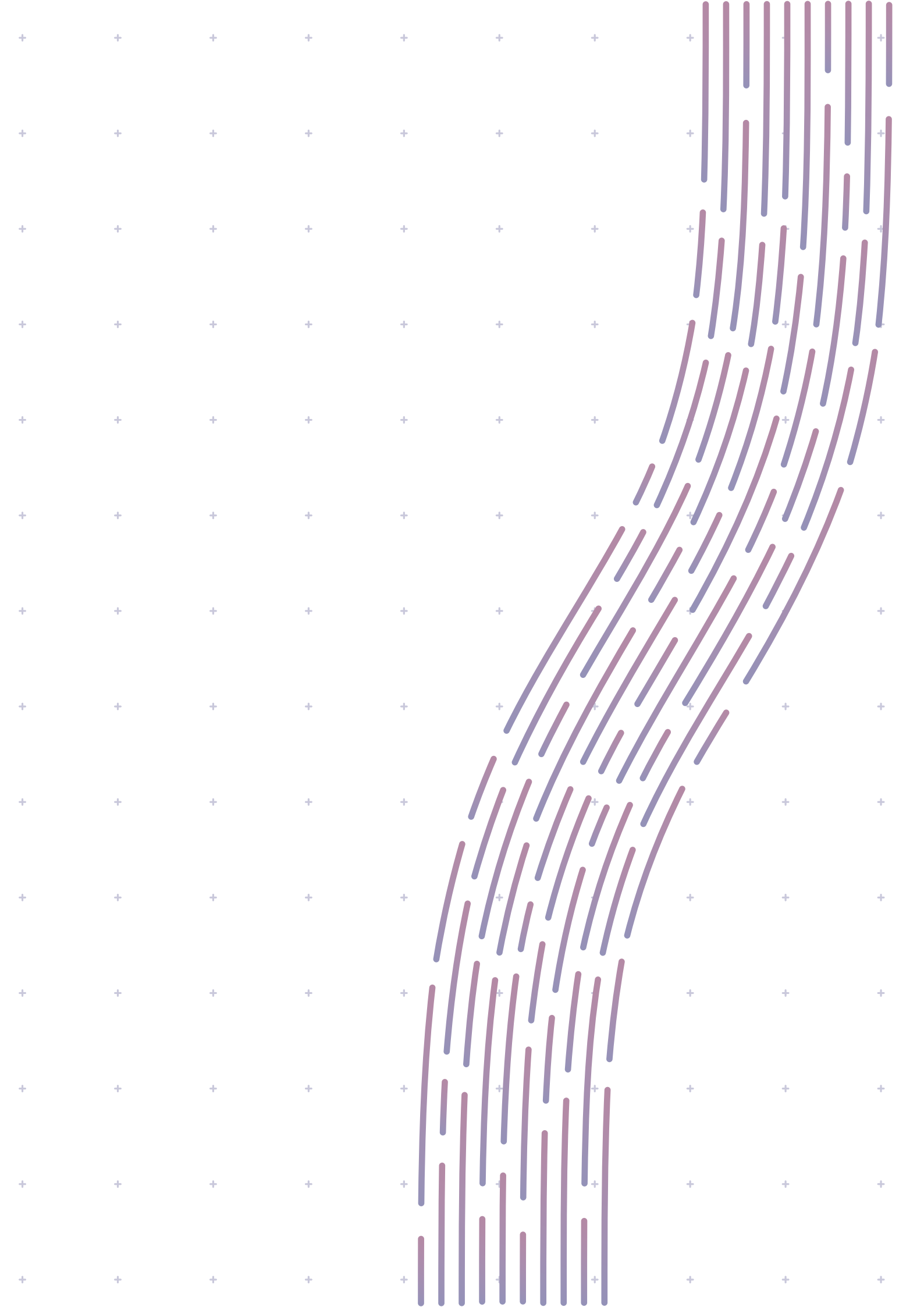
RÉPUBLIQUE  
FRANÇAISE

*Liberté  
Égalité  
Fraternité*



Plan stratégique  
de l'Agence nationale de la sécurité  
des systèmes d'information  
2025-2027

**Au cœur  
d'un collectif,  
pour une Nation  
cyber-résiliente**





« **L'action publique cyber requiert une évolution dans la gouvernance et la coordination des acteurs.** »

Depuis sa création, l'action de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a produit des progrès majeurs pour la cybersécurité en France. Ainsi, en une quinzaine d'années, la sécurité numérique des infrastructures critiques a été grandement améliorée, complexifiant drastiquement la tâche des attaquants voulant les atteindre. De même, l'offre de cybersécurité s'est fortement étoffée. Tous ces éléments sont essentiels pour contribuer à la confiance dans le numérique.

Pour autant, du fait d'un numérique toujours plus présent et essentiel et de la diversification de la typologie des attaquants, la menace cyber affecte dorénavant tous les pans de notre économie et de notre société. Cette évolution marque un tournant pour l'action de l'Agence, qui a pour mission d'organiser la protection et la réponse de la Nation face aux cyberattaques, dans un champ désormais bien plus large que celui des seules administrations de l'Etat et de leurs opérateurs critiques.

L'émergence de nouveaux acteurs publics et privés au sein de l'écosystème cyber contribue fortement à répondre à cet enjeu. Mais si étoffée qu'elle soit, l'offre industrielle de cybersécurité apparaît encore insuffisante, notamment pour répondre au besoin d'une offre dont le plus grand nombre pourra s'emparer avec simplicité et à moindre coût.

**Le plan stratégique de l'ANSSI pour 2025-2027 s'inscrit dans le cadre de la nouvelle stratégie nationale de cybersécurité pour la France.** Celle-ci

fixe un nouveau cap en termes de développement d'une résilience cyber collective, et notamment d'investissements technologiques, de renforcement de la cyberdéfense de la Nation, ou encore d'affirmation de notre puissance cyber au niveau international comme responsable et solidaire. Ce plan répond également à **une situation internationale toujours plus conflictuelle, dont les effets ont des répercussions toujours plus significatives dans le cyberspace.** Il intervient alors qu'une nouvelle mandature européenne démarre, avec au cœur de son agenda la sécurité de l'Europe et la mise en œuvre d'un nouveau cadre réglementaire (directive sur la sécurité des réseaux et des systèmes d'information (NIS 2), règlement sur la résilience cyber (CRA), règlement sur l'intelligence artificielle (RIA), etc.). Il s'inscrit enfin dans un contexte national et international qui exige de manière croissante **la prise en compte des enjeux sociétaux, tels que la question environnementale et l'impact du numérique sur le changement climatique.**

Dans ce contexte, l'action publique cyber requiert une évolution dans la gouvernance et la coordination des acteurs. L'Agence entend incarner cette évolution, en refondant ses modes d'interaction avec ses parties prenantes dans une logique de co-construction et en permettant au collectif national des acteurs de la cybersécurité d'amplifier leurs actions et leur impact. ●



# Les missions de l'ANSSI

Service du Premier ministre 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. La raison d'être de l'ANSSI est de construire et d'organiser, en interministériel, la protection de la Nation face aux cyberattaques, et de contribuer à la stabilité du cyberspace.

Son action s'inscrit dans le cadre des missions régaliennes de l'Etat, 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. Son action se traduit en cinq grandes missions : défendre, connaître, partager, accompagner, réguler.



## DÉFENDRE

- les systèmes d'information critiques de la Nation en concevant et opérant des capacités de détection des cyberattaques, et en garantissant la disponibilité de produits de sécurité de confiance capables de protéger les données les plus sensibles et de répondre aux menaces les plus élevées ;
- les victimes de cyberattaques et la Nation, en structurant au niveau national l'assistance aux victimes ;
- une vision autonome de la sécurité et de la stabilité du cyberspace au niveau international.



## CONNAÎTRE

- l'état de l'art en sécurité des technologies et des systèmes d'information ;
- les menaces et les risques dans le cyberspace ;
- les tendances du monde de la cybersécurité, en France, en Europe et à l'international.



## PARTAGER

- des recommandations, des méthodes et des outils aux acteurs de la cybersécurité et du numérique ;
- de la connaissance et des savoir-faire sur la menace et les réponses possibles, avec les partenaires techniques, opérationnels et stratégiques, qu'ils soient français, européens ou extra-européens ;
- largement son expertise pour renforcer la sécurité collective face aux risques cyber.



## ACCOMPAGNER

- le déploiement d'une politique publique en matière de cybersécurité et sa déclinaison territoriale ;
- les autorités dans leur compréhension du fait cyber ;
- les organisations régulées dans l'application des mesures de protection de leurs systèmes d'information et leurs réponses aux incidents ;
- la montée en compétence des administrations et du secteur privé par le développement des formations en cybersécurité ;
- le développement d'un écosystème de prestataires privés de produits et de services de confiance.



## RÉGULER

- la qualité des produits et services de cybersécurité au travers de démarches de qualification et de certification ;
- la qualité des produits embarquant des éléments numériques en promouvant la sécurité par conception et par défaut ;
- par la conception de dispositifs normatifs et réglementaires aux niveaux national, européen et international ;
- par le contrôle de leur bonne application.

# Amplifier et coordonner la réponse cyber face à la massification de la menace

La menace cyber concerne désormais tous les pans de notre société, des systèmes d'information les plus critiques de l'Etat et des collectivités territoriales, à ceux des TPE et PME, jusqu'aux équipements informatiques des citoyens. Face à cette massification, l'action publique a renforcé le cadre réglementaire cyber et accompagné l'essor de nouveaux acteurs de la cybersécurité : le Groupement d'intérêt public Action contre la cybermalveillance (GIP ACYMA), les centres de réponse à incident (CSIRT) sectoriels, territoriaux et ministériels, les prestataires privés, les unités dédiées à la cybersécurité des forces de sécurité intérieure et des forces armées, la section cyber du parquet de Paris, etc. Afin de continuer à renforcer les défenses du pays, l'ANSSI se donne pour priorité d'amplifier et de faciliter l'accès aux capacités de prévention et de réponse à la menace.

## → OBJECTIF 1

### Piloter la politique de résilience cyber de la France

Dans un contexte de menace renforcée, l'Etat doit faire évoluer son organisation et ses pratiques pour améliorer la résilience numérique de la Nation. L'ANSSI pilotera cette évolution en coordination avec les autres administrations et parties prenantes au niveau national et dans les territoires. Elle recherchera la cohérence avec la stratégie numérique de l'Etat, en s'appuyant sur un dialogue renforcé avec la direction interministérielle du numérique (DINUM). **L'Agence soutiendra une gouvernance renforcée de la cybersécurité de l'Etat, de concert avec le Centre de coordination des crises cyber (C4) et la chaîne de sécurité des systèmes d'information de l'Etat.** Dans ce cadre, elle soutiendra un investissement plus important sur les produits de sécurité régaliens destinés à protéger les communications les plus sensibles de l'Etat, et une refonte de la gouvernance associée. L'ANSSI accompagnera également la DINUM dans le déploiement d'outils sécurisés pour les agents de l'Etat et veillera à renforcer sa propre résilience cyber.

## → OBJECTIF 2

### Favoriser l'adoption du nouveau cadre de régulation cyber

En s'adressant à la fois aux fournisseurs et aux utilisateurs de solutions numériques, l'évolution du cadre réglementaire européen vise une élévation générale du niveau de cybersécurité de l'Union européenne. Ce faisant, il étend les missions des autorités nationales de cybersécurité en matière de contrôle et de surveillance de marché, et élargit considérablement le périmètre des organisations et produits régulés par ces autorités. **L'ANSSI aura pour priorité de préparer et d'accompagner ce changement d'échelle,** avec d'une part la mise en œuvre progressive de la directive NIS 2 et d'autre part l'application du CRA et la mise à jour des réglementations existantes (règlement sur la cybersécurité (CSA), règlement sur l'identification électronique et les services de confiance pour les transactions électroniques (eIDAS), en mettant notamment en place **la nouvelle mission de contrôle et supervision de l'Agence.** L'ANSSI profitera également de la réglementation NIS 2 pour **simplifier**

les règles de cybersécurité imposées au niveau national aux organisations régulées, et ainsi favoriser leur adoption. Elle s'investira à ce titre dans les travaux entre régulateurs nationaux visant cette simplification.

L'Agence mettra en œuvre une organisation adaptée pour s'assurer de prises de décisions impartiales dans les missions de contrôle, articuler au mieux ces missions avec les autres actions de l'ANSSI et maintenir un dialogue de confiance avec les acteurs régulés bénéficiant de l'assistance de l'Agence.

Ces missions seront complétées par la **structuration d'une offre de services plus lisible permettant d'articuler les accompagnements ciblés ou massifiés de l'ANSSI** (services d'audit automatisés, portail pour les entités régulées par NIS 2, formation en ligne, etc.). L'Agence mettra en œuvre une démarche de qualité et d'évaluation des impacts de ces services. Des indicateurs d'efficacité seront mis en place à cet effet et les retours de la part de ses bénéficiaires seront collectés et pris en compte.

### → OBJECTIF 3

## Défendre les systèmes d'information les plus critiques de la Nation

L'ANSSI renforcera et recentrera les capacités opérationnelles du centre national de réponse à incident, le CERT-FR, pour défendre les intérêts les plus fondamentaux de la Nation face à des attaquants stratégiques. Elle s'assurera que ses relais soient en mesure de porter des recommandations et actions efficaces pour que les acteurs puissent s'en saisir et se protéger. Dans la lignée des travaux entrepris pour les Jeux olympiques et paralympiques de Paris 2024 et dans ce cadre contraint, **l'Agence poursuivra l'adaptation du dispositif national de réponse à incident afin de préparer la Nation à gérer une crise d'ampleur.**

En matière de détection, il s'agira de faire évoluer ses infrastructures informatiques pour conforter ses

capacités et pour mieux répondre aux besoins de ses bénéficiaires, par exemple avec le déploiement d'un nouveau système de supervision interministériel, qui permettra de travailler plus étroitement avec les centres de réponse à incident des administrations, ce qui augmentera l'efficacité de la détection. Cela impliquera également une meilleure valorisation des données techniques que l'ANSSI recueille auprès de l'écosystème.

### → OBJECTIF 4

## Accompagner la structuration de l'écosystème cyber

Face à une menace cyber répandue, **l'Etat doit s'assurer que chaque entité ou citoyen, victime ou non, dispose d'un interlocuteur pertinent capable de répondre à ses besoins en cybersécurité**, avec un parcours d'assistance lisible et visible pour l'ensemble des entités et citoyens au niveau national et territorial.

Cela nécessite la mise en réseau et la coordination des acteurs qui font la cybersécurité pour **assurer la cohérence et l'efficacité du dispositif national** (administrations, GIP ACYMA, CSIRT, campus cyber, prestataires et fournisseurs de solutions privés), mais aussi **l'animation de communautés de parties prenantes** dans la mise en œuvre de l'action publique cyber (fournisseurs et utilisateurs). Au regard de leurs spécificités, l'Agence portera une attention particulière sur le développement d'écosystèmes et de services cyber locaux dans les territoires d'outre-mer.

Le développement de l'offre de services de l'ANSSI, de même que les innovations et transformations de ses modes d'action contribueront à soutenir l'action des acteurs de l'écosystème. Dans ce cadre, l'Agence cherchera à ouvrir et coconstruire ces solutions avec eux, ainsi qu'avec les acteurs publics de l'innovation et de la transformation, **en cohérence avec la politique de l'Etat en matière de développement de communs.** ●

# Développer les expertises indispensables pour contrer les menaces cyber

Entretenir un haut niveau d'expertise et préserver une maîtrise autonome des savoirs scientifiques et technologiques en matière de cybersécurité est indispensable pour garantir la cyberdéfense de la Nation, autant que sa souveraineté. La perpétuelle évolution de la menace cyber, l'évolution rapide des technologies du numérique ainsi que la transformation continue de la nature et du périmètre des systèmes d'information requièrent une adaptation permanente. Face à cet enjeu, l'ANSSI aura pour priorité de développer des expertises de pointe en lien avec ces évolutions et de partager le plus largement possible ses connaissances.

## → OBJECTIF 1

### Développer l'expertise sur les technologies à fort enjeu de cybersécurité

Le développement et le maintien à l'état de l'art des savoirs sur la sécurité des technologies numériques fait partie intégrante de la mission de l'ANSSI.

L'Agence renforcera dans ce cadre ses partenariats de recherche, notamment avec le Centre national de recherche scientifique (CNRS), le Commissariat à l'énergie atomique (CEA) et l'Institut national de recherche en informatique et automatique (INRIA).

Crucial au regard des défis majeurs posés par le développement potentiel, à moyen terme, d'un ordinateur quantique capable de remettre en cause les propriétés fondamentales de la cryptographie asymétrique, l'ANSSI finalisera et conduira **un plan de transition vers la cryptographie post-quantique**, en lien avec ses partenaires nationaux, européens et industriels.

Elle poursuivra sa montée en compétence sur les technologies du numérique les plus structurantes et, en particulier, ses travaux sur **les enjeux cyber des**

**technologies d'intelligence artificielle (IA)**. Elle sera en appui des autorités de surveillance de marché dans le cadre de l'application du règlement européen sur l'IA afin de les aider à évaluer les systèmes d'IA à haut risque et approfondira ses travaux sur l'utilisation de l'IA au service de la cybersécurité. L'Agence continuera aussi son investissement sur **le cloud**, compte tenu de l'augmentation de son usage par les administrations et les entreprises critiques. Elle devra notamment y adapter ses techniques d'audit, de détection et d'investigation numérique. Elle poursuivra par ailleurs son **accompagnement de la filière industrielle pour étoffer les offres de confiance**.

Le développement de ces expertises permettra en outre à l'ANSSI de diffuser des recommandations spécifiques afin d'accompagner les utilisateurs dans leurs usages de ces technologies et la transformation de leurs systèmes d'information.

→ OBJECTIF 2

## S'adapter aux évolutions techniques de la menace cyber

Depuis sa création, l'ANSSI est confrontée à une menace ciblée très sophistiquée, matérialisée par des attaquants fortement soutenus par des Etats et dont les objectifs principaux sont l'espionnage et la déstabilisation. L'Agence doit désormais faire face de surcroît à une menace devenue systémique, s'attaquant à tous les pans de l'économie et de la société, issue principalement de l'écosystème cybercriminel.

Les modes opératoires de ces attaquants sont en constante évolution et **l'ANSSI doit désormais traiter des attaques de plus en plus variées** comme le ciblage de téléphones portables professionnels comme personnels ou la compromission massive d'équipements de sécurité des systèmes d'information.

Face à cette menace, l'Agence aura pour priorité d'intensifier ses travaux de recherche et développement pour maintenir et approfondir son expertise technique d'analyse des modes opératoires adverses, d'audit de réseaux et de systèmes d'information, de détection d'attaques et d'investigation numérique. Elle aura également pour ambition de développer des méthodes plus automatisées pour s'adapter aux menaces de masse. Ces travaux seront réalisés en coopération avec ses partenaires nationaux et internationaux, en particulier dans son rôle de cheffe de file du C4.

→ OBJECTIF 3

## Accroître le partage de connaissances de l'ANSSI

Le partage de connaissances est essentiel pour renforcer la capacité de l'Etat et des organisations à se protéger contre la menace cyber. L'ANSSI visera ainsi à diffuser plus largement les connaissances et informations dont elle dispose, et à mieux valoriser les informations qui lui sont partagées.

L'Agence s'efforcera de produire et communiquer davantage de recommandations scientifiques, technologiques et opérationnelles, en particulier sur les sujets permettant de faire face à la menace. **Elle favorisera au maximum le partage en sources ouvertes de ses travaux et amplifiera les échanges d'informations opérationnelles au sein de communautés agréées** (InterCERT France, CSIRT relais, partenaires institutionnels et privés). Elle cherchera aussi à rendre ses recommandations plus accessibles à l'ensemble de ses bénéficiaires, notamment aux nouveaux acteurs régulés.

Ce partage de connaissances sera également orienté vers ses partenaires internationaux, dans la perspective d'une montée en compétence partagée. ●

## Promouvoir une action cyber européenne et internationale efficace

Les mandatures européennes précédentes ont mis en place les piliers de la cybersécurité européenne, en matière de gouvernance, de coopération et de réglementation. Au cours de la nouvelle mandature, ces différents piliers devront être consolidés et les capacités de l'Union européenne et de ses Etats membres devront poursuivre leur développement, afin de soutenir la dynamique du marché européen de la cybersécurité et d'élever les défenses de l'Europe. En tant que cheffe de file cyber pour la France, l'ANSSI portera cette ambition au sein des instances européennes comme auprès de ses partenaires européens. L'Agence promouvra par ailleurs les avancées européennes dans le cadre de ses échanges avec ses partenaires extra-européens et au sein d'instances internationales.

### → OBJECTIF 1

#### Accompagner une mise en œuvre harmonisée des réglementations cyber au niveau européen

Les réglementations et cadres adoptés ces dernières années (NIS 2, CRA, règlement sur l'IA, eIDAS, schéma de certification communs EUCC, etc.) constituent une avancée majeure pour la cybersécurité européenne. Toutefois, **leur pleine efficacité nécessite une coordination entre les Etats membres et une harmonisation de leurs exigences et de leur mise en œuvre.** A cette fin, l'ANSSI s'impliquera au niveau européen dans la définition des normes et le partage des bonnes pratiques nécessaires au succès de ces différentes réglementations, **en associant la communauté cyber française.** Elle participera également aux travaux visant à faire émerger une coordination européenne efficace entre régulateurs de la cybersécurité et du numérique.

### → OBJECTIF 2

#### Soutenir le développement d'un marché unique dynamique de solutions de confiance

Dans le cadre de la nouvelle mandature européenne, l'ANSSI s'impliquera fortement sur **la révision du règlement sur la cybersécurité (CSA)**, la certification européenne étant un outil clé pour apporter davantage de confiance et de transparence sur le niveau de sécurité des produits et services. Elle cherchera notamment à promouvoir le modèle français de certification de services et à renforcer le cadre existant, avec comme fort enjeu l'amélioration de son efficacité au travers de sa gouvernance. Dans cette perspective, elle veillera également à ce que ce cadre soutienne la diversité des offres au sein du marché unique, et à la bonne articulation des schémas nationaux et européens de certification. **Elle renforcera son action en tant qu'autorité nationale de certification de cybersécurité (ANCC)**

et partagera plus largement ses retours d'expérience avec ses partenaires extra-européens.

En parallèle, l'Agence soutiendra l'écosystème national de certification pour qu'il conserve sa place parmi les acteurs de premier plan au niveau européen, que ce soit en excellence ou en nombre de certificats émis.

### → OBJECTIF 3

## Promouvoir la coopération pour renforcer la résilience cyber européenne et internationale

Plusieurs réseaux de coopération cyber ont été créés ces dix dernières années afin de renforcer la coopération européenne et internationale en matière opérationnelle, de gestion de crise et de recherche et développement. **L'ANSSI est pleinement engagée dans ces réseaux de coopération dont elle a soutenu la création.** Au niveau européen, l'Agence, en tant que membre du réseau des centres nationaux de coordination (NCC), contribuera à orienter les programmes d'investissement européens Digital Europe et Horizon Europe vers les solutions et technologies clés pour la cybersécurité européenne. Elle continuera de s'investir pleinement dans la coopération européenne en matière de gestion de crise et de partage d'informations sur les incidents cyber, notamment au travers du réseau des CSIRT de l'UE (CSIRT Network) et du réseau CyCLONe (Cyber Crisis Liaison Organisation Network), qui ont fait la preuve de leur pertinence, et plus largement à l'international dans le cadre de différentes enceintes de coopération opérationnelle avec ses partenaires (OTAN, IWWN, etc.). Elle veillera également à **promouvoir l'organisation d'exercices de crise transnationaux**, s'appuyant sur les réseaux existants afin de renforcer la préparation des acteurs concernés.

### → OBJECTIF 4

## Encourager des formes nouvelles d'action publique cyber au niveau européen

Pour répondre aux enjeux de cybersécurité, dans un contexte réglementaire qu'il est nécessaire de stabiliser, **l'ANSSI soutiendra le développement de nouvelles politiques publiques au niveau européen, complémentaires au cadre législatif et normatif**, telles que le soutien au développement de services de cybersécurité de confiance, les actions visant au renforcement des compétences au sein des Etats membres à travers le soutien aux programmes de formation, le développement de la filière des centres d'évaluation des produits et services de cybersécurité, ou encore la mise en place de parcours de cybersécurité adaptés au niveau de maturité des organisations. Pour ce faire, elle s'appuiera sur le retour d'expérience des actions mises en place dans le cadre du plan France Relance, des Jeux olympiques et paralympiques de Paris 2024 ou encore dans le cadre de la sécurisation de secteurs spécifiques en France. ●

# Renforcer la prise en compte des enjeux sociétaux dans l'action de l'ANSSI

Le domaine de la cybersécurité n'échappe pas aux nombreux enjeux sociétaux contemporains : protection de l'environnement et transition énergétique, égalité femmes-hommes, inclusion, épanouissement professionnel, protection de la vie privée et des libertés publiques, etc. En tant qu'autorité nationale en matière de cybersécurité et de cyberdéfense, l'ANSSI a un devoir d'exemplarité dans la prise en compte de ces enjeux dans son domaine d'activité.

## → OBJECTIF 1

### Prendre en compte l'impact environnemental de la cybersécurité

Alors que l'impact environnemental du numérique (consommation énergétique et d'eau, raréfaction de certaines ressources, etc.) est désormais bien documenté, les enjeux environnementaux du sous-domaine de la cybersécurité restent peu explorés.

Dans la continuité des travaux qu'elle a conduits sur le reconditionnement des ordinateurs, **l'ANSSI renforcera ses connaissances en ce domaine et veillera à évaluer et maîtriser l'impact environnemental de ses recommandations.**

Cette préoccupation sera également mieux intégrée dans son organisation et son fonctionnement, en cohérence avec la politique environnementale des services du Premier ministre. A ce titre, elle effectuera un bilan carbone de ses activités et se fixera des objectifs concrets de réduction de son empreinte environnementale.

## → OBJECTIF 2

### Développer une politique ambitieuse de diversité

A l'instar de ce qui peut être observé plus généralement dans le secteur du numérique, **le domaine de la cybersécurité gagnerait à élargir son vivier de talents en faisant venir vers lui une plus grande diversité de profils** (notamment en termes de sexe, de situation de handicap ou d'origine sociale) et en soutenant une égalité de traitement dans le développement de leur carrière. L'action de l'ANSSI dans ce domaine se concentrera sur deux axes d'effort particulier.

En lien avec les autres acteurs impliqués (campus cyber, campus numérique, ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche, etc.), l'Agence poursuivra ses travaux en matière de sensibilisation et de formation aux métiers cyber, notamment à destination des publics qui en sont aujourd'hui les plus éloignés.

Elle évaluera par ailleurs de manière concrète la progression de la diversité en son sein afin de fixer des objectifs de progression des conditions permettant une plus grande diversité. Une politique spécifique de promotion du parcours de carrière

des femmes sera en particulier mise en œuvre. L'Agence portera aussi une attention renforcée à la représentation des femmes dans les événements publics auxquels elle s'associe.

### → OBJECTIF 3

## Informer et rendre compte des missions de l'ANSSI

L'ANSSI a régulièrement vu ses prérogatives renforcées par la mise en place de nouvelles réglementations (lois de programmation militaire successives, directives NIS 1 et 2, etc.).

Ces responsabilités invitent à l'application d'un **principe d'information et de transparence quant à la mise en œuvre des pouvoirs de l'Agence vis-à-vis de ses différentes parties prenantes**, et leur supervision par les autorités de contrôle indépendantes.

L'ANSSI veillera notamment à rendre compte publiquement de manière régulière et détaillée de son action et des moyens qui lui sont alloués, notamment au travers de ses rapports d'activité.

### → OBJECTIF 4

## Adapter le fonctionnement de l'ANSSI à l'évolution des usages du numérique et des organisations de travail

L'adoption d'outils et de méthodes adaptés à ses enjeux et à l'évolution des besoins de ses bénéficiaires sera une priorité pour l'ANSSI. D'une part, il s'agira de **garantir l'efficacité de l'action de l'Agence en améliorant le parcours de ses bénéficiaires** par des actions de simplification des démarches et de réduction des délais de traitement. D'autre part, l'Agence cherchera à apporter à ses agents **une meilleure qualité de vie au travail**, un équilibre des temps de vie personnels et professionnels, et une plus grande accessibilité, dans un contexte de télétravail et de fonctionnement multisite. ●







---

Version 1.0 – Mars 2025 – ISBN : 978-2-11167181-2

Licence Ouverte/Open Licence (Etalab — v2.0)

**AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**  
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP  
[www.cyber.gouv.fr](http://www.cyber.gouv.fr)

