RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RAPPORT D'ACTIVITÉ 2024

La montée en puissance de l'écosystème cyber

Sommaire

Édito de **Vincent Strubel**

2024 a été une année exceptionnelle pour l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ses équipes, dont je salue ici l'engagement profond au service de la protection de notre nation. Elle a été exceptionnelle, car nous avons réussi collectivement à faire des Jeux olympiques et paralympiques de Paris 2024 une fête. Si cet événement a fait l'objet d'un travail intense durant deux ans par toutes les sous-directions de l'ANSSI et « l'équipe de France » de la cybersécurité, il est aussi la consécration d'un modèle français de la cybersécurité qui, lui, a été enclenché depuis plusieurs années. Ce succès consacre la place de la France parmi les grandes nations de la cybersécurité. Nous en tirons de nombreux enseignements qui doivent nous permettre de gérer demain des crises de haute intensité.

Mais les Jeux olympiques et paralympiques sont l'arbre qui cache la forêt de 2024. Cette année, le dispositif de cyberdéfense national mis en place par l'Agence a également été éprouvé lors des élections européennes et législatives, à l'heure où des acteurs cherchent à déstabiliser ces temps forts démocratiques. L'ANSSI a par ailleurs poursuivi ses travaux de transposition de la directive NIS 2 qui sont le vecteur d'une transformation profonde de son organisation, de ses méthodes et de sa manière d'interagir avec ses bénéficiaires et ses partenaires. La nouvelle mission Contrôles et

Supervision constitue, à ce titre, un outil important pour l'Agence dans le nouveau contexte réglementaire cyber, et pas seulement pour NIS 2.

2024 a été aussi l'année de belles avancées européennes avec notamment le vote du règlement sur la résilience cyber que nous avons soutenu et qui constitue un pas important dans l'élévation générale de la cybersécurité de l'Union européenne. Elle a été aussi une année d'avancées techniques pour l'ANSSI, avec l'évolution de certains de nos référentiels, des coopérations internationales sur la transition vers la cryptographie post-quantique, ou encore un investissement fort sur des technologies d'avenir telle l'intelligence artificielle pour porter une voix rationnelle fondée sur des données scientifiques. Enfin, cette année a été aussi la première année où l'Agence a officiellement fonctionné sur quatre sites. Ce maillage au cœur de l'écosystème cyber français est un atout, dont nous constatons les bénéfices au quotidien.

Cette année exceptionnelle ouvre désormais la voie à une nouvelle étape pour l'ANSSI, qui a été partagée dans notre stratégie pour 2025-2027. Il s'agit de prendre acte des évolutions non seulement du paysage cyber, mais également de notre environnement plus global. Pour ce faire, nous aurons besoin de « l'équipe de France » de cybersécurité à nos côtés.

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).

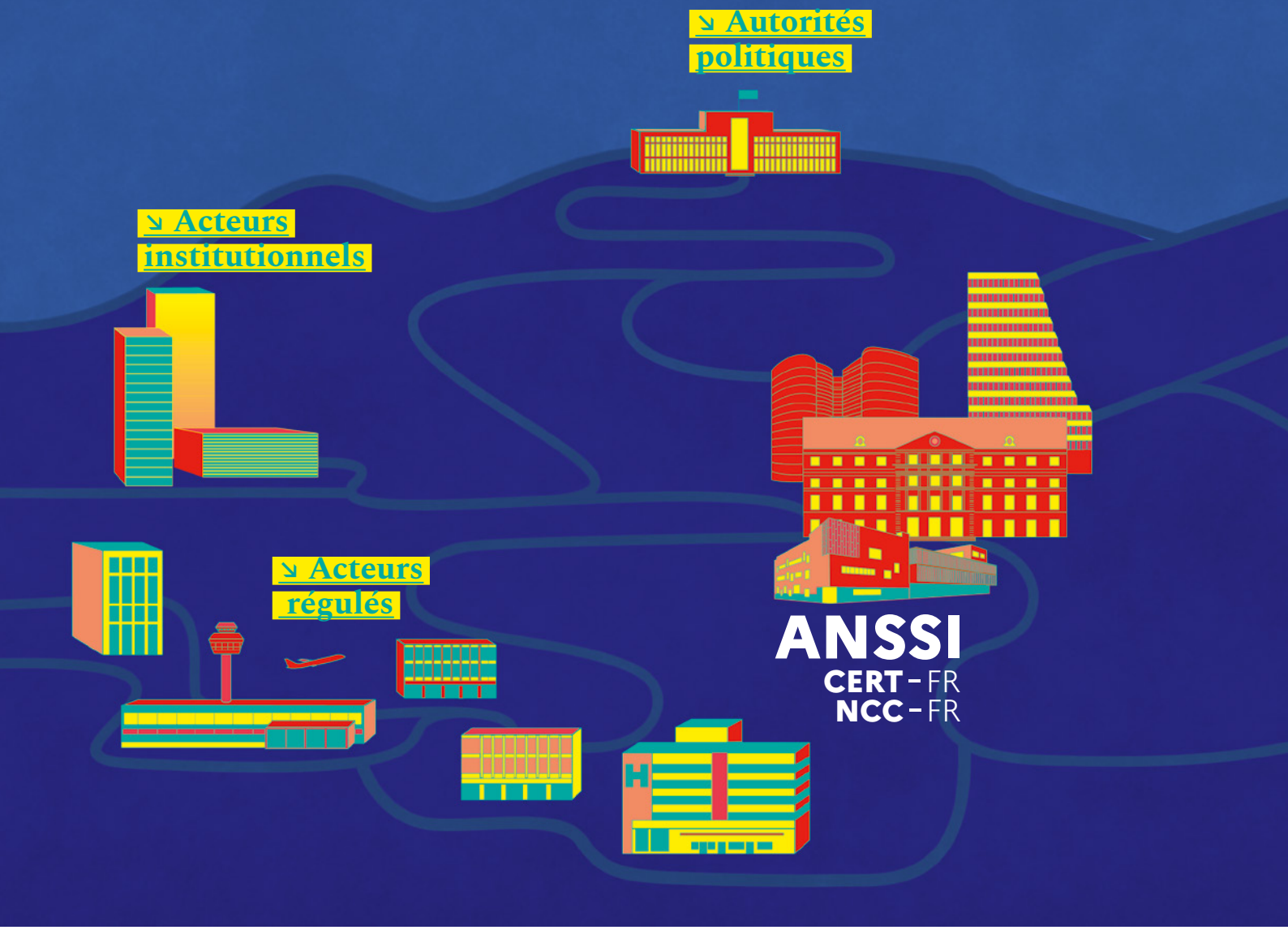
→ **La sous-direction Ressources** est responsable de la programmation et de l'exécution des activités de gestion et de pilotage des ressources financières, humaines, mobilières et immobilières, et de l'expertise et de l'accompagnement légal de l'ANSSI.

→ **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).

↘ Depuis 2023, une Agence sur quatre sites

L'ANSSI, auparavant répartie sur trois sites en Île-de-France, est présente sur quatre sites depuis l'inauguration d'ArteFact à Rennes en novembre 2023. Ces différentes implantations permettent à l'Agence d'être plus proche de ses bénéficiaires, de nouer des collaborations riches avec ses partenaires et de renforcer les synergies entre acteurs publics et privés.
Afin de prendre en compte les enjeux environnementaux inhérents au fonctionnement sur plusieurs sites, l'ANSSI a fait évoluer ses pratiques professionnelles : déploiement d'outils de visioconférence pour réduire les déplacements, dématérialisation de processus pour réduire la transmission de documents papier, mise en place de permanences sur site, désignation de correspondants (sécurité ou ressources humaines). Ces évolutions ont pour objectif de contribuer concrètement à la réduction des émissions carbone de l'Agence. Les enjeux concernant les conditions de travail sont également pris en compte, avec une attention particulière accordée aux temps de trajets entre les sites distants pour organiser des réunions en présentiel. Par ailleurs, le service créé en 2023 et dédié au pilotage des sites et de leurs bâtiments est monté en puissance en 2024 afin de répondre aux besoins soulevés par leur gestion. Il est le garant de leur bon fonctionnement, au bénéfice des agents y travaillant, sur les sujets d'infrastructures ainsi que de conditions de travail, et veille à une égalité de traitement des agents sur tous les sites. ●



Écosystème cyber

↘ 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.)
Organismes de normalisation (AFNOR, ETSI, etc.)

↘ Acteurs régulés

Administrations
OCE : Opérateurs de communication électronique
OIV : Opérateurs d'importance vitale
OSE : Opérateurs de services essentiels

↘ Autorités politiques

Élus locaux
Gouvernement
Parlement
Premier ministre
Président de la République
SGDSN : Secrétariat général de la défense et de la sécurité nationale

↘ Acteurs de la cyberdéfense

C4 : Centre de coordination des crises cyber (ANSSI, COMCYBER, DGA, DGSE, DGSI, MEAE)
CERT 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

↘ 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

↘ 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

↘ 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

2024 en chiffres

29,6
millions d'euros de budget (hors masse salariale)

4 386
événements de sécurité[2]
+ 15% par rapport à l'année 2023

59 191
rapports d'audits automatisés (ADS et SILENE)
+ 56% par rapport à l'année 2023

1 361
incidents[3]
+ 18% par rapport à l'année 2023

68
formations labellisées SecNumedu

117 856
attestations SecNumacadémie
+ 21% par rapport à l'année 2023

35
formations labellisées SecNumedu-FC

1 696
personnes formées au CFSSI[4]

[1] Personnels civils hors stagiaires et apprentis.
[2] Événements portés à la connaissance de l'ANSSI et qui ont donné lieu à un traitement par les équipes opérationnelles.
[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] Centre de formation à la sécurité des systèmes d'information.

Temps forts 2024

JANVIER

16 janvier
Publication du corpus de guides dédié à la remédiation des incidents de cybersécurité

31 janvier
Adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC)

FÉVRIER

Certification par l'ANSSI, au niveau élevé du règlement eIDAS, du moyen d'identification électronique de France Identité du ministère de l'Intérieur et des Outre-mer

Déploiement de la plateforme d'analyse de fichiers *Jecliqueoupas.cyber.gouv.fr* auprès des ministères

MARS

Publication des résultats de la deuxième relève du dispositif d'accompagnement des PME et start-up *cloud* vers une meilleure éligibilité à la qualification SecNumCloud

AVRIL

11 avril
Établissement du cadre européen relatif à une identité numérique

24 avril
Restitution des consultations auprès des fédérations professionnelles au sujet de la transposition de la directive NIS 2

29 avril
Publication du guide sur la sécurité des systèmes d'IA générative

MAI

3 mai
Restitution des consultations auprès des associations d'élus au sujet de la transposition de la directive NIS 2

8 mai
Arrivée sur le sol métropolitain de la flamme olympique, et début de la mobilisation de l'ANSSI dans le cadre des Jeux olympiques et paralympiques de Paris 2024

10 mai
Entrée en vigueur du décret d'application de la loi de programmation militaire 2024-2030, permettant à l'ANSSI de mettre en œuvre l'ensemble des nouvelles capacités dont elle l'a dotée

15 mai
Renouvellement de l'accord de reconnaissance mutuelle entre l'ANSSI et son homologue allemand, le BSI (*Bundesamt für Sicherheit in der Informationstechnik*), portant sur les certifications CSPN de l'ANSSI et BSZ du BSI

22 mai
Officialisation de la contribution de l'ANSSI au pilier *Trust* dans le cadre du Sommet pour l'Action sur l'IA prévu en 2025

JUIN

29 et 30 juin
Premier tour des élections législatives en France.
Accompagnement par l'ANSSI du ministère de l'Europe et des Affaires étrangères pour le vote par Internet des Français de l'étranger lors de ces élections

JUILLET

9 juillet
Publication des recommandations de l'ANSSI pour l'hébergement des systèmes d'information sensibles dans le *cloud*

Premiers prestataires de cybersécurité qualifiés « PACS » (prestataires d'accompagnement et de conseil en sécurité des systèmes d'information) par l'ANSSI

26 juillet
Cérémonie d'ouverture des Jeux olympiques

AOÛT

11 août
Cérémonie de clôture des Jeux olympiques

28 août
Cérémonie d'ouverture des Jeux paralympiques

SEPTEMBRE

8 septembre
Cérémonie de clôture des Jeux paralympiques et fin de la mobilisation de l'ANSSI

12 septembre
Lancement d'un nouvel appel à projets « Soutien aux PME et *start-up* pour renforcer leurs compétences dans le domaine de la cybersécurité » par l'ANSSI, dans le cadre de ses missions de Centre de coordination cyber français (NCC-FR), avec le Secrétariat général pour l'investissement (SGPI) et Bpifrance

30 septembre
Participation au sommet de la *International Counter Ransomware Initiative* (CRI), aux côtés des 67 autres pays

OCTOBRE

15 octobre
Présentation en Conseil des ministres du projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle du secteur financier dont le titre II, « Cybersécurité », vise à transposer la directive NIS 2

NOVEMBRE

20 novembre
Publication du règlement sur la cyber-résilience, ou *Cyber Resilience Act* (CRA), portant sur les exigences de cybersécurité pour les produits comportant des éléments numériques

20 novembre
Lancement de la plateforme MonAideCyber, permettant la fédération d'une communauté d'aidants cyber

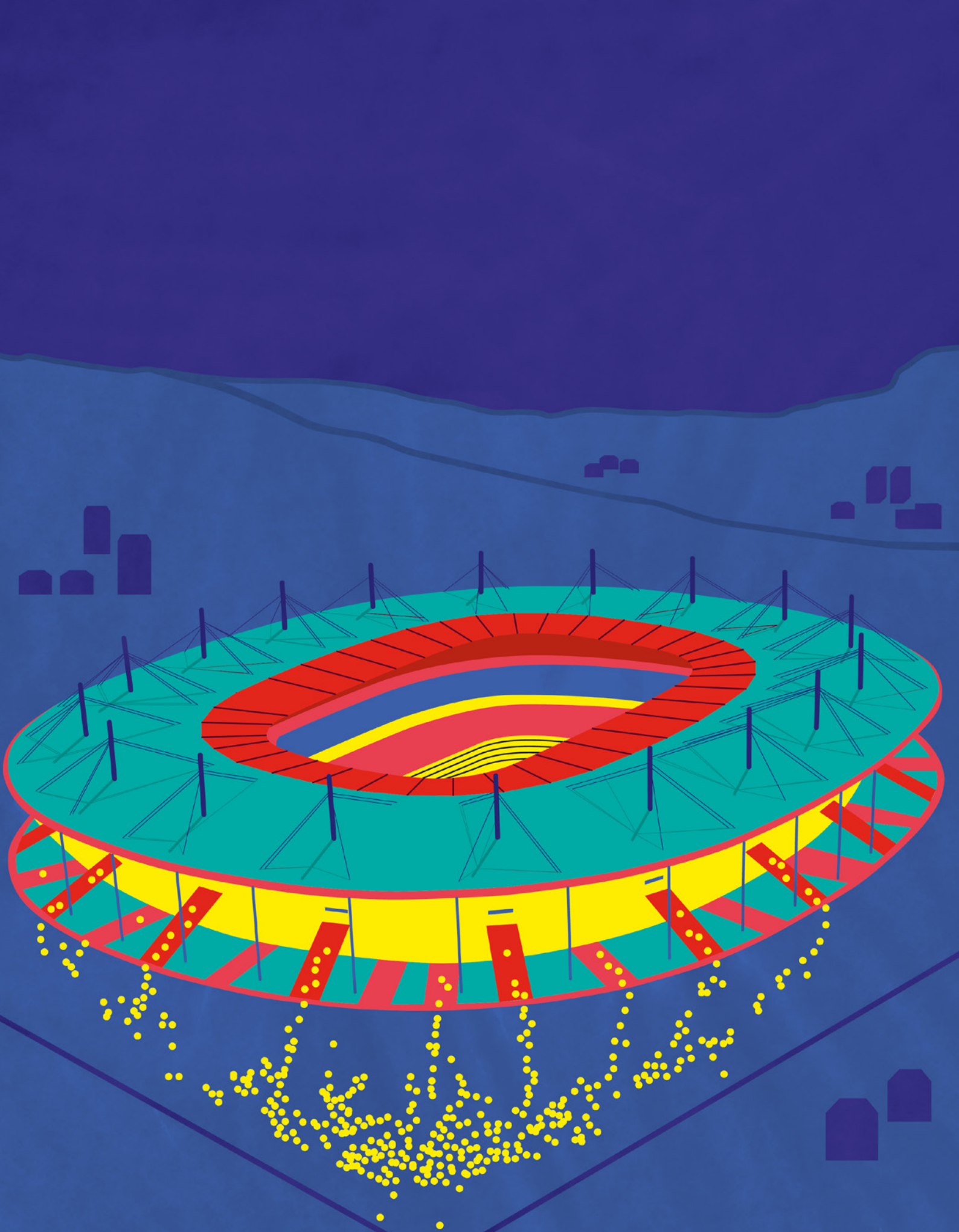
27 novembre
Publication de *Securing Tomorrow, Today : Transitioning to Post-Quantum Cryptography* avec le BSI

29 novembre
Publication des nouvelles versions des référentiels d'exigences permettant la qualification des prestataires d'audit de la sécurité des systèmes d'information (PASSI) et des prestataires de réponse aux incidents de sécurité (PRIS)

DÉCEMBRE

17 décembre
Lancement du 17Cyber, offrant une assistance en ligne pour toutes les victimes d'infractions numériques (particuliers, entreprises et collectivités)

18 décembre
Publication de *Guaranteeing the Cybersecurity of Major Sports Events Through Cooperation With the Private Sector* avec le BSI



Les Jeux olympiques et paralympiques de Paris 2024, un succès collectif

À la suite de la décision de la Première ministre le 20 juillet 2022, l'ANSSI s'est vu confier le pilotage de la stratégie de prévention des cyberattaques pendant les Jeux olympiques et paralympiques (JOP) de Paris 2024. En raison de leur exposition mondiale et des flux financiers importants qu'ils génèrent, les JOP constituent une cible de choix pour des attaquants aux motivations diverses. Dans son évaluation de la menace concernant les grands événements sportifs en France, publiée le 17 avril 2024, l'ANSSI rappelait que les Jeux olympiques précédents avaient été le théâtre de cyberattaques d'envergure : attaques par déni de service distribué (DDoS[5]) à Rio de Janeiro, sabotage à PyeongChang, et espionnage à Tokyo ont ainsi été observés. L'Agence évaluait les risques pesant sur la tenue de l'événement en prévoyant un niveau élevé de menace à motivation d'extorsion (escroqueries, vols de données), un niveau important de menace à visée de déstabilisation (sabotage, DDoS, défigurations de sites) et un niveau moyen de menace à but d'espionnage (ciblages de délégations étrangères ou de sous-traitants avec des données sensibles).

En tant que cheffe de file du volet cybersécurité dans la préparation et la conduite des JOP de Paris 2024, l'ANSSI s'est associée à l'ensemble des structures impliquées dans l'organisation des Jeux, dont en particulier la Délégation interministérielle aux Jeux olympiques et paralympiques (DIJOP), le ministère de l'Intérieur et des Outre-Mer (MIOM) et le Comité d'organisation des Jeux olympiques et paralympiques (Paris 2024). Le dispositif mis en place s'est décliné en cinq axes : connaissance de la menace, sécurisation des systèmes d'information critiques, protection des données sensibles, sensibilisation de l'écosystème, et préparation opérationnelle intensive.

[5] *Distributed Denial of Service :* Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. L'action peut être malveillante ou être la conséquence d'un mauvais dimensionnement du service. On parle de « déni de service distribué » lorsque l'attaque fait intervenir un réseau de machines (souvent compromises) afin d'interrompre le ou les services visés.

L'anticipation des Jeux, la préparation d'un écosystème

La mise en place de cette stratégie a débuté par l'identification de l'écosystème JOP, réalisé avec le soutien de la Coordination nationale pour la sécurité des Jeux (CNSJ) du ministère de l'Intérieur et des Outre-mer et de Paris 2024. L'ANSSI a pu cibler près de 500 entités impliquées dans les Jeux, réparties en catégories selon leur criticité, afin de déployer auprès d'elles une stratégie de sécurisation préventive en amont de l'événement. Afin de fournir un accompagnement efficace, l'Agence s'est en particulier efforcée de bien comprendre les activités et les métiers associés aux JOP – accréditation, billetterie, gestion des accès aux sites, diffusion audiovisuelle, transport des accrédités, lutte anti-dopage, etc. – et d'en saisir les enjeux de sécurité, développant ainsi une connaissance fine des entités accompagnées et défendues.

> « Le but était de beaucoup parler de cybersécurité avant les Jeux pour en parler le moins possible pendant. »
>
> Vincent Strubel, directeur général de l'ANSSI

La stratégie de sécurisation préventive comprenait quatre volets. Le volet diagnostic consistait, au travers d'une centaine d'audits de cybersécurité, à identifier les vulnérabilités présentes sur les systèmes d'information et à élaborer des plans de sécurisation. En complément, 80 entités ont pu accéder aux services d'audits automatisés de l'Agence.

Des marqueurs de renseignement sur les menaces cyber, ou *Cyber Threat Intelligence* (CTI), ont été partagés avec environ 130 entités et une assistance de détection a été offerte à une dizaine d'entités majeures. Le volet sécurisation proposait des accompagnements techniques pour la plupart des entités auditées. Le volet contrôle concernait, quant à lui, plusieurs dizaines d'entités, dont des sites de compétition, ayant fait l'objet d'audits de contrôle visant à s'assurer de la bonne mise en place des mesures de sécurité. Enfin, le volet détection consistait en un déploiement, au bénéfice de quelques entités particulièrement critiques, d'un service de détection de cyberattaques, sous la forme d'EDR (*Endpoint Detection and Response*) managé et de sondes industrielles.

Simultanément, un plan de sensibilisation au bénéfice de l'ensemble de l'écosystème des Jeux a également été mis en œuvre à partir de l'année 2023. Il a permis d'informer sur la menace cyber à l'encontre des grands événements sportifs et de diffuser de nombreuses recommandations et bonnes pratiques de cybersécurité. Ce plan s'est traduit par plusieurs sensibilisations réalisées par les délégués territoriaux de l'ANSSI dans les régions et les coordinateurs sectoriels de l'Agence, ainsi que par un séminaire organisé le 5 juillet 2023 au Campus Cyber. Sa mise en œuvre a également consisté en la diffusion de plusieurs rapports présentant une évaluation de la menace, et d'une campagne d'emailings thématiques. ●

2 000

heures d'expertise en sécurité consacrées à l'accompagnement d'une dizaine d'entités critiques, au bénéfice du ministère de l'Intérieur et des Outre-mer, de Paris 2024, de ses partenaires les plus importants et d'acteurs étatiques.

↘ Des exercices de crise cyber pour s'entraîner et entraîner l'écosystème

L'ANSSI s'est engagée dans une série d'actions visant à accompagner les principaux acteurs publics et privés associés aux JOP dans leur sécurisation informatique et la résilience de leur organisation en cas d'attaque cyber. Plusieurs exercices de crise ont été organisés en 2023 et en 2024 pour se préparer collectivement à réagir en cas de cyberattaques lors des Jeux. En complément, des kits d'exercice « clé en main » ont été proposés aux acteurs de l'écosystème des JOP 2024 – territoires hôtes, pouvoir publics, fournisseurs de service, sites de compétition – souhaitant s'entraîner à partir d'un scénario adapté à leur niveau de maturité. Au total, les organisations ont pu choisir parmi 12 formats d'exercices (quatre types de secteurs déclinés en trois types d'exercices selon le niveau de maturité). Des centaines d'entités ont donc pu bénéficier d'un exercice de crise cyber adapté à son contexte, et progresser sur les enjeux de réponses à incident et de continuité de service essentielle dans le cadre des Jeux. ●

Une coordination cyber orchestrée par l'ANSSI

L'Agence a défini, en coopération avec les différents services de l'État impliqués dans la préparation des JOP, un dispositif renforcé de veille, d'alerte et de traitement des événements de cybersécurité. Ce dispositif exceptionnel de coordination interministérielle s'est incarné dans le Centre national de commandement stratégique (CNCS). Il comprenait notamment une posture spécifique destinée à supporter une activité opérationnelle accrue. L'ANSSI a été identifiée comme point d'entrée unique des signalements cyber, permettant ainsi la centralisation de l'information et l'optimisation du traitement des incidents. Tous les événements de cybersécurité identifiés ont ainsi été signalés à l'Agence, via Paris 2024, l'interministériel ou l'écosystème des Jeux, dans le but de consolider une vue unique de la situation cyber des JOP.

De plus, une coordination rapprochée avec l'organisateur de l'événement, via la présence d'un officier de liaison de l'ANSSI auprès des équipes cyber de Paris 2024, a été mise en place pour faciliter les remontées et la qualification des événements de cybersécurité. Par ailleurs, les partenaires nationaux et internationaux de l'Agence ont été sollicités et mobilisés de manière régulière en amont des JOP afin de garantir la coopération dans le cadre de cet événement international. Durant l'événement, l'information cyber liée aux JOP a fait l'objet d'un partage régulier avec les partenaires internationaux, tant de manière bilatérale que dans le cadre de dispositifs dédiés, en particulier le Centre de coopération internationale (CCI), le réseau européen de gestion de crise EU-CyCLONe et le réseau des CSIRT de l'Union européenne (CSIRTs Network). D'un point de vue opérationnel, face au risque de cyberattaques d'ampleur ou ciblant de multiples sites sur le territoire national, des procédures permettant de recourir en urgence à des renforts issus d'autres administrations de l'État (en particulier au sein du ministère des Armées et du ministère de l'Intérieur et des Outre-mer, avec lesquels des conventions ont été signées) ont été mises en place. ●

↘ Le CERT-FR, toujours plus accessible

En amont des Jeux et dans la perspective de faciliter le signalement d'événements de cybersécurité au CERT-FR, l'Agence a continué à améliorer ses services et canaux de communication. Destinés à simplifier les procédures et les échanges avec ses bénéficiaires, ils visent à leur fournir un accompagnement optimisé dans les situations de crise.
Les travaux se sont poursuivis au-delà des Jeux, et jusqu'en 2025 :
→ Le nouveau numéro de téléphone court 3218 a été mis en place pour assurer en 24/7 un accès facilité et résilient au CERT-FR.
→ Le portail Internet Club SSI a été refondu et mis en production en novembre 2024. Il s'enrichira en 2025 de nouveaux services comme le pré-enregistrement des futures entités soumises à la réglementation NIS 2. ●

« Il n'est pas possible d'improviser des réponses en plein milieu d'une catastrophe. La préparation, l'outillage et l'entraînement sont indispensables pour maintenir l'activité en cas de cyberattaque. On l'a fait pour les JOP, et ça marche. »

Cédric Mullot, chargé de mission cyber entraînement, sous-direction Opérations

Le déroulement des Jeux, un accomplissement pour l'écosystème et l'Agence

Aboutissement de deux ans de travaux, l'ensemble de cette stratégie de prévention, planifiée au long cours par l'Agence, a porté ses fruits. La préparation de l'écosystème et le dispositif opérationnel mis en œuvre ont permis qu'aucun événement cyber n'affecte la tenue des cérémonies d'ouverture et de clôture ou les épreuves des JOP. Si un total de 548 événements de cybersécurité a été recensé par l'ANSSI entre le 8 mai, arrivée de la flamme à Marseille, et le 8 septembre 2024, date de la cérémonie de clôture des Jeux paralympiques, leur impact a été faible ou nul. Ces événements se décomposent en 465 signalements[6] et 83 incidents. Sur les types d'événements de cybersécurité rapportés, près de la moitié des événements de cybersécurité correspondent à des indisponibilités dont un quart sont dues à des attaques par DDoS. Le reste des événements de cybersécurité représente des tentatives de compromission ou des compromissions, des divulgations de données ou bien encore des signalements de vulnérabilités. Sans surprise, les secteurs d'activité les plus ciblés se sont avérés être les entités gouvernementales, le sport, le divertissement (sites de compétitions et Paris 2024) et les télécommunications.

Ainsi, si l'Agence et ses partenaires nationaux ont accompagné plusieurs victimes dans la résolution d'incidents, les événements de cybersécurité survenus au cours de cette période ont été caractérisés par leurs faibles impacts. Cette absence de crise cyber majeure, consécration de plusieurs années de préparation pour l'ANSSI et l'écosystème des Jeux, a permis à la France de démontrer sa résilience en matière de cybersécurité et de conforter son rang à l'international. Le travail engagé a également rendu possible la mise en place d'un cadre pérenne pour la gestion de crise majeure. L'écosystème cyber national en est sorti renforcé en termes de coordination et d'action commune. En résumé, les JOP ont été un succès pour l'Agence, mais surtout un succès collectif de l'écosystème. ●

[6] Événements de sécurité d'origine cyber avec un impact faible pour le système d'information de la victime, requérant une intervention minimum de l'Agence.

« Comme pour nos athlètes olympiques, la cybersécurité des Jeux olympiques et paralympiques s'est préparée sur le temps long, bien avant le coup d'envoi. Et derrière chaque performance, il y a une équipe entière qui fait tourner la machine. »

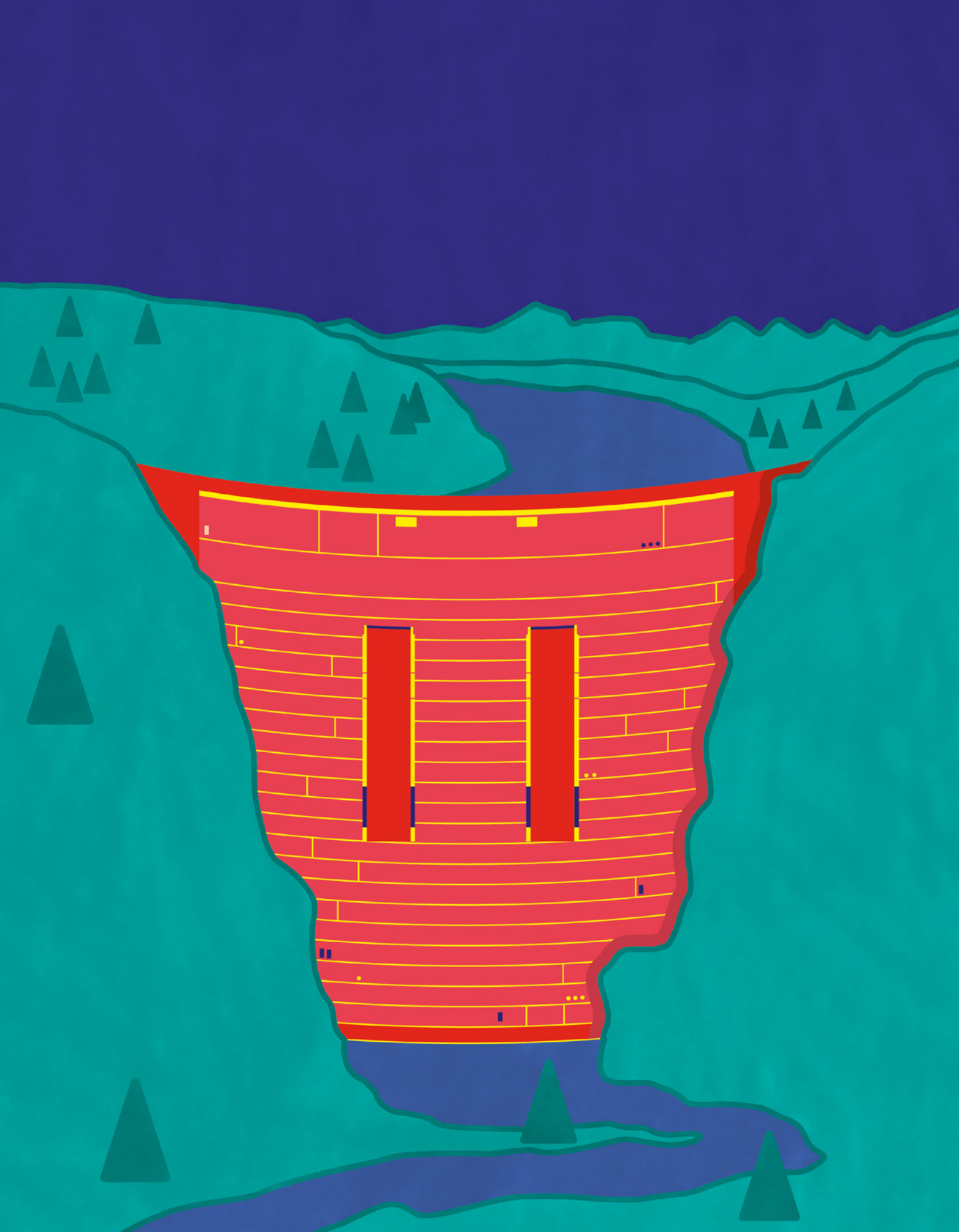
Julien Garcin, chargé de mission gouvernance, sous-direction Ressources

548

événements de cybersécurité ayant affecté des entités en lien avec l'organisation des Jeux olympiques et paralympiques de Paris 2024 ont été rapportés à l'ANSSI entre le 8 mai et le 8 septembre 2024 :

465 signalements

83 incidents



Un cadre réglementaire en pleine mutation pour élever le niveau global de cybersécurité

En 2024, les travaux de sécurisation du cyberespace se sont poursuivis à l'échelle de l'Union européenne (UE) et de la France, concrétisant progressivement les différents projets réglementaires et législatifs auxquels l'Agence a collaboré ces dernières années.

L'ANSSI mobilisée pour la transposition de la directive NIS 2

Enjeu majeur de l'Agence en 2024 et pour les années à venir, la directive NIS 2 (*Network and Information Security*, sécurité des réseaux et des systèmes d'information en français) vise à renforcer le niveau de cybersécurité des tissus économique et administratif des pays membres de l'UE. Alors que la première directive NIS visait à protéger les acteurs économiques majeurs de l'UE, cette nouvelle directive élargit le champ des entités et secteurs concernés et introduit des exigences plus adaptées, notamment au regard du renforcement de la menace cyber. Les exigences prévues par la directive européenne inviteront plusieurs milliers d'entités à renforcer leurs moyens de cyberdéfense, avec pour objectifs un fonctionnement structurel plus sûr, davantage de confiance vis-à-vis de leurs parties prenantes et une meilleure compétitivité pour les entreprises. En France, l'ANSSI a été chargée de piloter la transposition de la directive et d'assurer sa mise en œuvre.

« CRA, REC, NIS 2, CSA, LPM… Ce sont autant d'acronymes qui ont pour but d'améliorer le niveau de cybersécurité nationale et européenne et de défendre notre souveraineté et les intérêts des entreprises et des citoyens. »

Adeline Lescaut, cheffe de la division Expertise et accompagnement légal, sous-direction Ressources

La directive NIS 2 concerne les administrations de l'État, les collectivités territoriales, et les moyennes et grandes entreprises qui interviennent dans 18 secteurs d'activité. Elle distingue deux catégories d'entités régulées, les entités essentielles (EE) et les entités importantes (EI). La directive prévoit pour les entités trois actions, dont les exigences résultant de la transposition en droit français seront proportionnées au type d'entité (entité essentielle ou importante) et aux risques qu'elles supportent : fournir et mettre à jour un certain nombre d'informations à l'autorité nationale, mettre en place des mesures juridiques, techniques et organisationnelles pour gérer les risques qui menacent la sécurité de leurs réseaux et de leurs systèmes d'infor-

mation et déclarer à l'autorité nationale leurs incidents de sécurité ayant un impact important. De ce fait, la directive NIS 2 engage et redéfinit les rôles 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 directive.

Cette transposition, extrêmement dimensionnante pour l'ANSSI, a donc fait l'objet de multiples travaux au cours des mois écoulés, au-delà de la rédaction du volet cyber du projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle du secteur financier, qui a été déposé au Parlement en vue de son examen le 15 octobre 2024. Le titre II « Cybersécurité », du projet de loi dit « Résilience », vise à transposer la directive NIS 2 et à adapter le droit national à la suite de l'entrée en vigueur des règlements eIDAS (*Electronic Identification, Authentication and Trust Services*[7]) et CSA (*Cybersecurity Act*[8]).

Dans une logique de co-construction, l'ANSSI a organisé des consultations auprès des fédérations professionnelles concernées, des associations d'élus locaux et des ministères. Il s'est agi de prendre en compte les réalités et les besoins des futures entités régulées pour faire aboutir les travaux de transposition. L'Agence a coordonné le travail d'élaboration du projet de loi et les négociations sur le règlement d'exécution NIS 2 au niveau européen[9].

En parallèle, l'ANSSI développe sa stratégie d'accompagnement et propose une offre de services dédiée via la plateforme *Monespacenis2.cyber.gouv.fr*, actuellement en version bêta, sur laquelle les entités peuvent effectuer un test leur permettant de savoir si elles sont concernées par la directive, et à quelle catégorie elles appartiennent. Cette plateforme d'information vient compléter une démarche de communication et de sensibilisation des entités aux exigences à venir, afin de leur en faciliter la prise en main. L'Agence s'est préparée à accompagner plusieurs milliers d'entités dans leur démarche d'enregistrement comme entité régulée, tout en adaptant ses outils pour être en capacité de recueillir leurs signalements et de travailler en coopération avec les partenaires territoriaux et internationaux. ●

[7] Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

[8] Règlement relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications.

[9] Voir *digital-strategy.ec.europa.eu*

« La directive NIS 2 est la clé de notre résilience collective face aux risques cyber. Elle ouvre la porte à une avancée majeure, tant pour notre sécurité numérique que pour notre souveraineté. »

Mathieu Couturier, chef de la division Management de la sécurité numérique, sous-direction Stratégie

↘ La création de la mission Contrôles et Supervision

Face au constat d'une augmentation dans le domaine de la sécurité des systèmes d'information des réglementations, notamment européennes, prévoyant un rôle de supervision et de contrôle, l'ANSSI a lancé en 2022 un projet visant à proposer une organisation interne revue pour mieux exercer les pouvoirs de contrôle et de supervision qui lui sont confiés. Ce travail a abouti, en tout début d'année 2025, à la création de la mission Contrôles et Supervision, structure séparée des sous-directions et directement rattachée au directeur général de l'Agence. Elle aura la charge de réaliser les missions de contrôle au titre du dispositif Sécurité des Activités d'Importance Vitale (SAIV) établi par la loi de programmation militaire de 2013, du règlement eIDAS ou encore du règlement sur la cybersécurité (CSA) pour ce qui concerne la certification européenne en matière de cybersécurité. Elle est également engagée dans les travaux préparatoires de la mise en œuvre de la supervision et du contrôle au titre de la directive NIS 2. Il est prévu que la préparation des mesures correctrices que l'ANSSI pourrait prescrire à l'encontre des entités qui ne se conforment pas aux exigences prévues par ces textes relève de la mission. ●

« Le *Cyber Resilience Act* est le pendant de la directive NIS 2 pour les fournisseurs de solutions numériques. Il a été pensé en miroir de NIS 2 pour permettre une juste répartition de l'effort sur l'élévation du niveau de cybersécurité européen entre les fournisseurs de solutions numériques et les organisations soumises à la réglementation NIS 2. »

Sylvain Leroy, chef de la division Produits et services de sécurité, sous-direction Expertise

Le règlement sur la cyber-résilience ou *Cyber Resilience Act*, complémentaire à la directive NIS 2

Si NIS 2 fixe pour objectif de sécuriser les réseaux et systèmes d'information des entreprises et administrations de l'UE, le *Cyber Resilience Act* (CRA) vise quant à lui à sécuriser les produits numériques utilisés dans l'UE par les organisations et le grand public. Ce règlement européen, publié le 20 novembre 2024, définit ainsi 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.

En 2024, l'Agence a participé à l'aboutissement des négociations du règlement au niveau européen et entamé des travaux de mise en œuvre du CRA. Dans cette perspective, un projet a été lancé au sein de l'ANSSI pour organiser le signalement des vulnérabilités et des incidents, contribuer aux travaux européens de définition de normes et d'exigences, définir les processus d'évaluation nécessaires et préciser l'organisation nationale. L'Agence prévoit également d'accompagner l'écosystème dans la mise en œuvre de cette nouvelle réglementation. ●

La révision du règlement européen eIDAS, vers un cadre de confiance pour l'identité numérique

Le règlement eIDAS, ou règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, a pour objectifs de faciliter la sécurité des transactions numériques transfrontalières et de créer un cadre de confiance pour l'identité numérique et l'authentification. Après la publication de la première version du règlement n° 2024/1183 en juin 2014, la Commission européenne a initié une révision du texte en vue d'en améliorer l'efficacité, d'en développer les cas d'usage quotidiens, d'inclure plus largement le secteur privé et de promouvoir une identité numérique fiable pour tous les citoyens européens.

En appui de la Direction interministérielle du numérique (DINUM), cheffe de file de la négociation, l'ANSSI a participé aux travaux de révision du règlement européen. Plaidant pour une plus forte prise en compte des aspects de cybersécurité, l'Agence a activement contribué aux groupes de travail réunissant les principaux experts des États membres pour accompagner la Commission européenne dans la mise en œuvre technique du règlement. Le texte de révision eIDAS, qui vise à permettre à tous les citoyens européens de disposer d'une identité numérique d'ici 2030, a pu ainsi entrer en vigueur le 20 mai 2024.

Parmi les innovations majeures apportées par ce texte, figure l'introduction d'un portefeuille européen d'identité numérique. Il est désormais imposé aux États membres de mettre à disposition de leurs citoyens des portefeuilles européens d'identité numérique reconnus dans l'ensemble de l'UE d'ici novembre 2026. Ceux-ci permettront à leurs utilisateurs de stocker des données d'identification (nom, prénom, lieu et date de naissance, etc.) ou des justificatifs liés à leur identité (adresse postale, diplômes, etc.), de les communiquer aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et hors ligne, sur des services publics ou privés dans toute l'Europe. Le texte a également permis l'élaboration et la mise à jour de l'architecture de référence des portefeuilles, dite « ARF ».

Par ailleurs, le périmètre de services de confiance[10] est désormais élargi avec quatre nouveaux services pouvant faire l'objet d'une qualification : la délivrance d'attestation électronique d'attribut, l'archivage électronique, les registres électroniques et la gestion à distance des dispositifs de création de signature et cachet électronique qualifiés. En France, l'ANSSI est l'organe de contrôle chargé de qualifier les prestataires de services de confiance, ainsi que d'établir et de tenir à jour la « liste de confiance ».

Enfin, cette révision instaure la création d'une nouvelle instance de coopération européenne transverse pour assister la Commission dans ses travaux et assurer le suivi de la mise en œuvre de la réglementation : l'*European Digital Identity Cooperation Group* (EDICG). Aux côtés de la DINUM, l'ANSSI participera à ce nouveau groupe de coopération afin de favoriser la prise en compte des enjeux de cybersécurité. ●

L'EUCC, premier schéma de certification européen de cybersécurité en application

Le 31 janvier 2024, la Commission européenne a annoncé l'adoption de l'EUCC (*EU Common Criteria*[11]), premier schéma de certification européen conforme aux réglementations européennes en matière de cybersécurité. Entré en vigueur en février 2024, il prévoit la délivrance des premiers certificats un an plus tard. Le schéma EUCC fournit des règles et procédures de certification harmonisées à l'échelle de l'UE pour les produits des technologies de l'information et de la communication et reprend les caractéristiques des différents schémas de certification nationaux rassemblés au sein de l'accord de reconnaissance mutuelle du *Senior Officials Group – Information Systems Security* (SOG-IS). En tant que représentante de la France au sein du Groupe européen de certification de cybersécurité (ECCG), l'ANSSI a activement contribué à la conception de ce schéma, développé dans le cadre du règlement européen *Cybersecurity Act* (CSA).

En octobre 2024, l'ANSSI a déposé un dossier auprès du Comité Français d'Accréditation (COFRAC) pour devenir le centre de certification national pour la délivrance des certificats EUCC. Une fois l'accréditation obtenue, l'ANSSI deviendra l'Autorité nationale de certification de cybersécurité (ANCC), chargée de délivrer les certifications pour le niveau élevé et de surveiller la bonne application du schéma EUCC en France. Les certificats SOG-IS existants pourront être réévalués en certificats EUCC dès lors que les nouvelles exigences seront respectées. Ce schéma sera également un support important à la mise en œuvre des évolutions récentes du cadre européen sur la cybersécurité. Ces exigences s'inscrivent dans la lignée de celles prévues par la directive NIS 2 et la révision du règlement eIDAS. ●

[10] Voir https://cyber.gouv.fr/les-services-de-confiance

[11] *The European Common Criteria-based cybersecurity certification scheme*, ou schéma européen de certification de cybersécurité fondé sur des critères communs.

↘ La Loi de programmation militaire 2024-2030 : de nouvelles capacités opérationnelles pour l'ANSSI

Les JOP de Paris 2024 ont constitué un « test » de changement d'échelle opérationnel réussi, notamment grâce aux nouvelles capacités dont l'Agence a été dotée par la Loi de programmation militaire (LPM) 2024-2030, promulguée le 1er août 2023. Le décret d'application des articles L. 2321-2-1 à L. 2321-4-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques, ainsi que des arrêtés tarifaires qui en découlent, ont été publiés le 10 mai 2024, suivi par la publication du décret sur le traitement automatisé des données à caractère personnel le 19 juillet 2024. Cette entrée en vigueur a marqué l'aboutissement de près de trois ans de travail pour permettre à l'ANSSI de disposer de capacités opérationnelles supplémentaires d'anticipation, de caractérisation et de neutralisation de la menace.
Plus précisément, ce travail a permis à l'Agence d'accroître sa connaissance des modes opératoires des cyberattaquants, de mieux remédier aux effets de leurs attaques et d'alerter plus efficacement les victimes des incidents ou des menaces pesant sur leurs systèmes d'information. L'ANSSI a ainsi pu développer ses capacités de prévention et de caractérisation de la menace via le filtrage *Domain Name System* (DNS)[12], la collecte de cache DNS, ou encore un recueil de données significativement amélioré. Enfin, un meilleur traitement des vulnérabilités produit oblige désormais les éditeurs à notifier les vulnérabilités significatives à l'ANSSI et à leurs clients.
L'Agence a mené les travaux d'opérationnalisation des dispositifs octroyés par la LPM 2024-2030 tout en maintenant une logique de cohérence avec les dispositifs déjà mis en place par les opérateurs, hébergeurs ou fournisseurs de résolveurs DNS.
Les moyens mis en œuvre ont été présentés à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) dans le cadre de son contrôle des opérations de l'ANSSI.
Le déploiement de ces dispositifs s'est fait en plusieurs phases, avec une capacité opérationnelle initiale atteinte avant les JOP et ayant permis d'assurer la prévention contre la menace et les vulnérabilités pendant l'événement. Ce déploiement se poursuivra jusqu'en 2026, avec une intégration progressive de nouvelles capacités et de nouveaux acteurs sollicités. ●

↘ La stratégie nationale de cybersécurité : pour une résilience cyber de premier rang

En 2018, le Premier ministre confiait au secrétaire général de la défense et de la sécurité nationale (SGDSN) la réalisation d'une revue stratégique de cyberdéfense, soit le premier grand exercice de synthèse stratégique dans ce domaine. Ce document marquait le début d'une stratégie fondée sur le durcissement de la protection des systèmes informatiques de l'État et des organismes d'importance vitale, ainsi que sur le renforcement de la sécurité numérique pour les citoyens, les institutions et l'ensemble des acteurs qui participent du dynamisme économique, industriel, social et culturel de la France.
En 2024, l'ANSSI a activement contribué à la réalisation de la stratégie nationale de cybersécurité, dont le pilotage a été confié à Bruno Marescaux, adjoint au délégué général de l'armement, et le secrétariat assuré par le SGDSN.
Cette stratégie 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. ●

[12] Le filtrage des systèmes de nom de domaine est une solution de protection contre les usages malveillants des noms de domaine.

L'expertise de l'ANSSI pour anticiper les nouveaux enjeux technologiques

L'évolution des technologies implique de nouvelles opportunités pour les défenseurs comme pour les attaquants. Qu'ils concernent l'hébergement de données dans le *cloud*, le développement de l'intelligence artificielle (IA), ou encore la cryptographie post-quantique, les travaux de l'ANSSI visent à maintenir un haut niveau de maîtrise de l'environnement technique des bénéficiaires et à anticiper les impacts des nouveaux usages technologiques sur la sécurité des systèmes d'information.

Sensibiliser l'écosystème aux enjeux de cybersécurité de l'intelligence artificielle (IA)

L'Agence travaille sur l'IA tant à des fins de sécurisation des systèmes d'IA que d'identification des opportunités et des menaces représentées par ces derniers pour la cybersécurité. Le développement de l'IA soulève des enjeux cyber (la cybersécurité de l'IA ; par l'IA ; face à l'IA) que l'ANSSI intègre dans son plan d'actions. L'Agence souhaite s'inscrire dans la continuité de la stratégie nationale en IA, qui a pour objectif de tirer le meilleur parti de l'IA sur le plan cyber, en accompagnant le développement en France d'une IA de confiance, sécurisée et responsable, qui bénéficie davantage à la cyberdéfense qu'aux cyberattaquants.

Pour ce faire, l'ANSSI promeut une approche par les risques, la valorisation des règles cyber existantes et l'élaboration de nouvelles règles adaptées aux spécificités des systèmes d'IA. En 2024, l'Agence a structuré ses travaux en matière d'IA afin de répondre à plusieurs enjeux soulevés par ces technologies : l'adoption rapide de l'IA par les bénéficiaires de l'ANSSI, l'entrée en vigueur du règlement européen sur l'IA, l'émergence progressive d'une gouvernance internationale de l'IA, et le besoin de la part tant de l'écosystème IA que cyber, de recommandations de cybersécurité spécifiques et de schémas de certification dédiés. Par ailleurs, l'Agence s'implique dans la stratégie nationale sur l'IA (financée via le plan d'investissement France 2030), afin d'accompagner la montée en maturité des start-up et des projets de recherche dans ce domaine.

La publication du guide *Recommandations de sécurité pour un système d'intelligence artificielle (IA) générative* sur le compte LinkedIn de l'ANSSI a suscité

4 470
réactions

1 045
republications
et

15 947
clics en faisant le succès d'audience le plus important de l'Agence sur la plateforme en 2024

« L'ANSSI a vocation à sensibiliser l'écosystème aux enjeux de cybersécurité liés à l'IA, à accompagner le déploiement d'une IA de confiance sur le marché, ainsi qu'à apporter son expertise à l'échelle européenne sur la mise en œuvre de la réglementation et l'élaboration de schémas de certification dédiés. »

Hugo Mania, chef de projet IA, sous-direction Expertise

Le récent engouement pour les produits et services d'IA générative, dont certains sont rendus facilement accessibles au grand public, a entraîné des réflexions au sein des organisations publiques et privées afin d'étudier les éventuels gains de productivité qui pourraient en découler. Si cette technologie offre de nouvelles perspectives, il convient d'adopter une posture de prudence lors de son déploiement et de son intégration dans un système d'information existant. Dans une perspective de sensibilisation de l'écosystème aux enjeux de cybersécurité liés à ces technologies, l'ANSSI a publié en avril 2024 le guide *Recommandations de sécurité pour un système d'intelligence artificielle (IA) générative*. Ce document s'intéresse à la sécurisation d'une architecture de système d'IA générative et vise à sensibiliser les administrations et entreprises aux risques liés à ce type d'outil. Il promeut les bonnes pratiques à mettre en œuvre depuis la phase de conception et d'entraînement d'un modèle d'IA jusqu'à la phase de déploiement et d'utilisation en production.

En octobre 2024, l'Agence et son homologue allemand le BSI ont publié leurs *Recommandations de sécurité concernant les assistants de programmation basés sur l'IA*. Ce document conjoint présente les opportunités et les risques de l'utilisation d'assistants de programmation basés sur l'IA, notamment les risques liés aux services mutualisés, accessibles depuis Internet. La publication a pour objectif de contribuer à une utilisation responsable et sûre de ces outils et propose une série de recommandations de sécurité à destination des responsables et des développeurs. ●

La cryptographie post-quantique : un enjeu de sécurité majeur

Le développement potentiel, à moyen terme, d'un ordinateur quantique capable de remettre en cause les propriétés fondamentales de la cryptographie asymétrique, pourrait faire effondrer la sécurité de la cryptographie à clé publique largement déployée pour sécuriser les infrastructures numériques. La menace d'attaques rétroactives (dites *store now, decrypt later*) nécessite une prise en compte de ce risque dès aujourd'hui, avant même de savoir si le développement d'un tel ordinateur quantique sera réalisable.

La cryptographie post-quantique, ou *post-quantum cryptography* en anglais (PQC), consiste en un ensemble d'algorithmes cryptographiques comprenant les établissements de clés et les signatures numériques et assurant une sécurité contre la menace quantique, en plus d'offrir une sécurité face aux attaques classiques. Pour l'ANSSI, la cryptographie post-quantique représente la voie la plus prometteuse pour se prémunir contre la menace quantique. Cette transition vers la cryptographie post-quantique durera plusieurs années et impactera l'intégralité de l'écosystème du numérique. Sa réussite à l'échelle nationale et européenne est un enjeu majeur de la prochaine décennie.

L'Agence a mené en 2024 et poursuit actuellement des travaux pour proposer des orientations de transition réalistes et actionnables. L'ANSSI a défini deux axes stratégiques de travail : premièrement, garantir la disponibilité d'une offre de produits PQC de confiance, c'est-à-dire accompagner le développement d'une offre de produits de sécurité intégrant une nouvelle génération d'algorithmes cryptographiques qui résistent à l'ordinateur quantique ; deuxièmement, accompagner la migration des systèmes d'information des bénéficiaires de l'Agence.

« Pour se protéger contre la menace quantique, la France a besoin d'accélérer le développement de son offre de produits de confiance intégrant de la cryptographie post-quantique. »

Samih Souissi, chef d'État-major de la sous-direction Expertise

Concernant le premier axe, l'ANSSI a publié fin 2024 les résultats d'une enquête menée auprès de 18 développeurs de produits de cybersécurité intégrant de la cryptographie. *Cette enquête* a permis d'identifier plusieurs freins techniques et organisationnels à traiter dans le cadre de la transition : le manque de maturité de la technologie, le manque de briques logicielles de référence, l'inquiétude sur les performances, l'absence de marché immédiat, le faible nombre d'experts, etc. Ces freins représentent autant d'axes de travail à mener pour l'Agence. En complément de cette démarche, un travail a été mené auprès des centres d'évaluation de la sécurité des technologies de l'information (CESTI) pour s'assurer qu'ils seront en mesure d'instruire le sujet de la cryptographie post-quantique sur les produits qui leur seront soumis pour évaluation. Le centre de certification national (CCN) a initié les premiers projets pilotes d'évaluation et a également mis à jour sa doctrine d'agrément cryptographique. Enfin, dans le but de décliner et de faire évoluer la doctrine technique, l'Agence a initié des études sur l'intégration de la cryptographie post-quantique dans les protocoles ainsi que des réflexions sur des recommandations autour de la cryptoagilité[13].

Dans le cadre du second axe, l'ANSSI a publié une *enquête* sur l'offre de prestations d'accompagnement et de conseil en PQC en France. Menée auprès d'une trentaine de prestataires, elle a permis d'identifier leurs attentes ainsi que les freins qu'ils rencontrent. Pour la sphère publique, l'Agence a également consulté une cinquantaine de ministères et d'entreprises stratégiques qui devront déployer des produits incluant de la cryptographie post-quantique, afin de mesurer leurs connaissances sur le sujet. Pour améliorer la compréhension de cet enjeu par les bénéficiaires de l'ANSSI, le centre de formation à la sécurité des systèmes d'information (CFSSI) propose depuis début 2024 une formation dédiée à la cryptographie post-quantique. Enfin, une analyse de risque quantique a été initiée dans le but de prioriser les cas d'usage et les secteurs qui devront s'inscrire dans une démarche de transition.

L'Agence travaille également de concert avec ses homologues européens sur la cryptographie post-quantique. En janvier 2024, l'ANSSI a publié avec ses homologues allemand (le BSI), néerlandais (la Netherlands National Communications Security Agency), et suédois (la Swedish National Communications Security Authority), *un position paper sur la distribution quantique de clé (quantum key distribution ou QKD)*. Cette publication vise à aider les décideurs et les responsables politiques à porter un jugement éclairé sur les apports potentiels et les limites de la QKD. Elle conclut qu'une priorité claire doit être donnée à la migration vers la cryptographie post-quantique pour répondre à la menace quantique. L'Agence a également cosigné *une importante déclaration conjointe* avec 17 autres États membres de l'UE, préconisant de déployer dès maintenant et en priorité des solutions de cryptographie post-quantique hybrides. Par ailleurs, l'ANSSI copréside avec ses homologues allemand et néerlandais le *workstream* PQC du groupe de coordination NIS qui a pour objectif de définir la feuille de route de la transition vers la cryptographie post-quantique en Europe au sein de l'Union européenne.

[13] La cryptoagilité est la capacité d'un équipement à pouvoir évoluer pour mettre à jour ses algorithmes cryptographiques.

↘ Data-centric Security (DCS), une nouvelle approche pour accéder de manière sécurisée aux données

L'approche nommée *Data-centric Security* (DCS) vise à renforcer la sécurisation des données elles-mêmes en considérant que, peu importe où se trouve l'information, elle doit être sécurisée. Cette nouvelle approche, guidée par les nouveaux usages comme celui de la mobilité ou par les technologies comme le *cloud*, conduit à revisiter les architectures classiques des systèmes d'information.
L'ANSSI et l'Institut national de recherche en informatique et automatique (INRIA) ont engagé des échanges techniques sur le sujet en 2024 visant à définir les mécanismes cryptographiques répondant aux exigences de sécurisation de ces nouvelles architectures. ●

↘ Sécuriser l'hébergement dans le *cloud* des systèmes d'information sensibles

Le *cloud* représente un enjeu majeur pour la protection des données et des systèmes d'information les plus sensibles. L'état de la menace démontre que les attaquants ont, depuis plusieurs années, identifié les offreurs de solutions *cloud* et leurs infrastructures comme des cibles d'intérêt pour la conduite de cyberattaques.
En accord avec la doctrine « *cloud* au centre » de l'État, l'ANSSI a publié une série de recommandations de sécurité pour l'hébergement des systèmes d'information sensibles dans le *cloud*, répondant à un besoin partagé par ses bénéficiaires. En effet, face au recours croissant des technologies de *cloud computing* par les secteurs privés et publics, l'Agence a souhaité mettre à disposition des recommandations qui indiquent, en fonction du type de système d'information, de la sensibilité des données et du niveau de la menace, les types d'offres *cloud* à privilégier. Elles précisent également les cas d'usage pour lesquels l'ANSSI préconise l'utilisation de solutions qualifiées SecNumCloud, qui garantissent un haut niveau d'exigence tant du point de vue technique, qu'opérationnel ou juridique.
Sous la forme d'un *livret* complété d'une *foire aux questions*, cette série de recommandations de l'Agence constitue un outil d'aide à la décision pour les entités qui envisagent un hébergement *cloud* pour leurs systèmes d'information de niveau de diffusion restreinte, les systèmes d'information sensibles des opérateurs d'importance vitale et des opérateurs de services essentiels, ainsi que des systèmes d'information d'importance vitale (SIIV). ●

Travailler avec l'écosystème cyber pour accompagner un nombre toujours plus important de bénéficiaires

Face à l'évolution de la menace cyber, devenue systémique et ciblant l'ensemble du tissu économique et social, de nouvelles mesures de cyberdéfense ont été engagées ces dernières années, et en particulier en 2024, à l'échelle européenne et française. Les moyens à la disposition de l'État, et notamment ceux de l'ANSSI ont été renforcés au travers des diverses réglementations (LPM 2024-2030, NIS 2, CRA, CSA, eIDAS, etc.). Dans ce changement d'échelle, l'écosystème cyber joue un rôle clé, en particulier dans l'accompagnement des milliers d'entités concernées par la directive NIS 2 sur le territoire français. Il est soutenu par l'ANSSI dans son rôle de coordinatrice de l'écosystème cyber. •

Renforcer le développement d'offres de cybersécurité de confiance

Les usages ne cessant d'évoluer, les organisations doivent pouvoir recourir à des solutions de sécurité qui protègent efficacement les données et les systèmes d'information. La politique industrielle de l'ANSSI s'attache à favoriser le développement et la pérennité d'offres privées adaptées aux enjeux de sécurité pour permettre le renforcement de la cybersécurité de l'État, des collectivités territoriales et des acteurs privés. Cette approche nécessite un suivi des acteurs de l'industrie et de l'innovation dans le domaine de la cybersécurité et une coordination avec les administrations porteuses de politiques industrielles pour mettre en place des leviers d'action efficaces.

La liaison entre l'échelon européen et national, désormais nécessaire, s'est notamment concrétisée au travers du réseau des Centres de coordination nationaux (les « NCC ») présents dans chaque État membre de l'UE, et sur lesquels s'appuie l'action du Centre de compétences cyber européen (ECCC). L'ANSSI a été désignée pour incarner sa déclinaison française, le NCC-FR. Ce centre répond aux exigences du règlement (UE) 2021/887 visant à favoriser l'expertise, la recherche et les capacités industrielles en matière de cybersécurité au sein de l'Union européenne. En juillet 2024, l'Agence a formé un consortium avec Bpifrance, la banque publique d'investissement et opérateur des programmes d'innovation nationaux et européens, pour la phase d'opérationnalisation du NCC-FR. Cette phase, d'une durée de 24 mois, bénéficie d'un soutien financier de l'UE et permettra d'atteindre une pleine capacité opérationnelle à l'horizon 2026. Le NCC-FR assure trois missions : la promotion et l'accompagnement des appels à projets européens en cours, le développement d'appels à projets nationaux, et l'animation de l'écosystème cyber. Le NCC-FR rend ainsi visibles et lisibles les dispositifs de soutien européens à l'écosystème, notamment financiers, qui sont permis par les programmes européens Horizon Europe et Digital Europe. Le centre permet d'identifier des possibilités de consortiums public-privé entre les fournisseurs/prestataires, les centres de recherche et les organismes fédérateurs en régions pour répondre aux grands projets européens à venir. Ensemble, Bpifrance et le NCC-FR proposent

un accompagnement aux entreprises pour les aider à préparer leurs candidatures aux appels à projets européens. Au cours de l'année 2024, le NCC-FR a développé un programme de soutien financier pour encourager les start-up, scale-up, PME et/ou entreprises de taille moyenne (ETI) à adopter ou à développer l'innovation numérique, à renforcer la sécurité de leurs offres et à monter en compétences. L'appel à projets « Soutien aux PME et start-up pour renforcer leurs compétences dans le domaine de la cybersécurité » a ainsi été lancé en septembre 2024 par l'ANSSI, le secrétariat général pour l'investissement en charge de France 2030 et Bpifrance, pour un montant total de 2 millions d'euros.

L'Agence s'attache par ailleurs à améliorer la coordination et la synergie entre les acteurs de l'écosystème. Ainsi, les interactions et travaux avec la communauté cyber française se sont développés tout au long de l'année 2024, en s'appuyant sur l'expertise de l'Agence et sur ses réseaux institutionnels et industriels. Les interlocuteurs de l'ANSSI sont notamment les administrations françaises porteuses de politiques industrielles ou d'innovation, les fournisseurs de produits et prestataires de services de cybersécurité et leurs fédérations professionnelles, le Campus Cyber, les plateformes régionales de services, les centres de recherche, ou encore des utilisateurs. L'Agence permet la diffusion des connaissances et bonnes pratiques dans la communauté et l'amélioration continue du niveau de sécurité des solutions de cybersécurité disponibles sur le marché. ●

Développer et améliorer l'offre de Visas de sécurité ANSSI

Dans le domaine des certifications et qualifications, démarches qui visent à identifier par un Visa de sécurité les offres de cybersécurité de confiance, l'ANSSI a qualifié en 2024 les cinq premiers prestataires d'accompagnement et de conseil en sécurité des systèmes d'information (PACS). Publié en 2023, le référentiel PACS a pour objectif d'assister les responsables de la sécurité des systèmes d'information et leurs équipes dans leurs missions de protection des systèmes d'information, et notamment d'homologation de sécurité, de gestion des risques, de conception d'architectures sécurisées, et de préparation à la gestion de crises d'origine cyber.

Dans une démarche d'amélioration continue, l'Agence a publié le 29 novembre 2024 les nouvelles versions des référentiels d'exigences permettant la qualification des prestataires d'audit de la sécurité des systèmes d'information (PASSI) et des prestataires de réponse aux incidents de sécurité (PRIS). Lancés en 2022, les travaux de mise à jour se sont basés sur le recueil auprès de l'écosystème (prestataires, commanditaires, centres d'évaluation) de leurs besoins et propositions. À ce titre, plusieurs groupes de travail thématiques et deux appels publics à commentaires ont été organisés. Ces nouvelles versions améliorent significativement le déroulement des prestations en apportant plus de souplesse et en prenant mieux en compte les contraintes opérationnelles. Elles introduisent la notion de niveaux de qualification : un prestataire peut ainsi désormais réaliser des prestations qualifiées au niveau substantiel ou élevé. Une prestation de niveau élevé permet d'avoir, par rapport au niveau substantiel, une garantie renforcée sur la compétence du prestataire, la confiance que l'on peut lui accorder et sa capacité à protéger les informations et supports relatifs à la prestation. Les nouvelles versions des référentiels PASSI et PRIS seront traduites en anglais afin de les promouvoir auprès de la Commission européenne qui étudie actuellement l'opportunité, au titre du règlement européen *Cybersecurity Act*, de créer les schémas de certification des PASSI et PRIS au niveau européen.

Par ailleurs, la qualification SecNumCloud, qui identifie des prestataires de *cloud* de confiance, s'est développée en 2024. En effet, la liste des 27 lauréats de la deuxième relève du dispositif d'accompagnement des PME et start-up *cloud* vers une sécurisation accrue et une meilleure éligibilité à la qualification SecNumCloud a été publiée. L'offre de *cloud* qualifiée SecNumCloud s'est étendue et comprenait 14 solutions de 7 offreurs fin 2024. Parallèlement, 8 sociétés ont engagé un processus de qualification SecNumCloud. ●

[14] Prestataires de détection d'incidents de sécurité.

[15] Prestataires d'administration et de maintenance sécurisées.

↘ L'animation de la communauté des offreurs cyber qualifiés

Au cours de l'année 2024, l'ANSSI a consolidé et intensifié ses activités d'animation des communautés d'offreurs détenant un Visa de sécurité ANSSI. Ces communautés visent à assurer le maintien de la qualité et des compétences ainsi que l'accessibilité de l'offre de confiance. Les ateliers organisés par l'ANSSI dans ce cadre ont pour objectif de faire monter en compétences les communautés de prestataires et coconstruire des initiatives. L'approche s'adresse, pour le moment, aux prestataires de services de cybersécurité de confiance (plus précisément les qualifiés PASSI, PACS, PRIS, PDIS[14], PAMS[15]). En 2024, 10 consultations et 16 ateliers ont été organisés avec ces prestataires et l'écosystème industriel. Les échanges ont alimenté les travaux de mise à jour des référentiels de l'ANSSI, ont permis de coconstruire des recommandations, de partager les bonnes pratiques existantes, ou encore de renforcer les compétences en réponse à incident, en conseil, en audit, et en remédiation. En complément, les ateliers ont facilité l'intégration des principes et exigences des référentiels de l'ANSSI. Le nombre de prestataires PRIS a doublé en un an, et le nouveau référentiel PACS a reçu plus de 15 candidatures en 2024. ●

↘ Le corpus de guides dédié à la remédiation des incidents de cybersécurité

Face à la nécessité de renforcer la compétence de l'écosystème cyber en remédiation post-incident, l'ANSSI a démarré en 2022 des travaux sur le sujet, impliquant un grand nombre d'experts. La rédaction d'un corpus organisé en trois volets (technique, opérationnel, stratégique) a fait l'objet d'un appel à commentaires auprès de l'écosystème cyber en 2023. Celui-ci a permis de prendre en compte les retours des offreurs et des bénéficiaires afin de publier officiellement une première version des trois guides remédiation en janvier 2024. Le corpus a vocation à être alimenté et mis à jour de manière continue. Cette publication a permis de lancer une véritable démarche d'animation de la communauté des acteurs de la remédiation. Sur une période d'un an et demi, six ateliers ont été organisés avec les PRIS, avec pour objectif d'échanger sur les bonnes pratiques en remédiation, mais aussi de réfléchir aux prochaines publications à intégrer dans le corpus. En parallèle, l'Agence a participé à un grand nombre de groupes de travail et d'événements cyber pour diffuser les principes de ces guides. ●

Les CSIRT relais, un réseau d'assistance essentiel

Issus d'un projet du plan France Relance en 2021, et soutenus dans leur création par l'ANSSI, les CSIRT (*Computer Security Incident Response Team*) territoriaux sont des centres de réponse aux incidents cyber implantés dans les territoires. Ils traitent les demandes d'assistance des acteurs dans leurs territoires et les mettent en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques. Ces CSIRT territoriaux, déployés progressivement ces dernières années, fournissent localement un service de réponse à incident de premier niveau gratuit, complémentaire à celui proposé par les prestataires, par la plateforme *cybermalveillance.gouv.fr* et le dispositif 17Cyber et par les services du CERT-FR.

Ils accompagnent les bénéficiaires dans le processus de judiciarisation de leurs incidents en les guidant pour déposer plainte auprès des services de police ou de gendarmerie. En complément, ils les aident à faire les déclarations auprès de la Commission nationale de l'informatique et des libertés (CNIL) lorsque la situation l'exige. Les CSIRT territoriaux portent également des missions de prévention, de sensibilisation et d'accompagnement dans la montée en maturité des acteurs de leurs territoires. Ce dispositif est un service de proximité qui apporte une réponse aux problématiques de cybersécurité dans les territoires. Les CSIRT territoriaux connaissent les besoins et les spécificités de leur écosystème local et travaillent main dans la main avec les acteurs et les

dispositifs nationaux. Ils communiquent au CERT-FR les incidents qui ont lieu sur leur territoire. Les CSIRT se font également les relais de dispositifs tels que MonAideCyber ou Cyber PME.

Sur la période du 1er janvier 2024 au 18 décembre 2024, les 12 CSIRT territoriaux implantés dans l'hexagone ont ainsi porté à la connaissance de l'ANSSI près de 700 événements de sécurité numérique dont 400 incidents. Certains de ces incidents ont pu gravement affecter le fonctionnement de l'entité. C'est notamment le cas lors d'attaques par rançongiciel, qui ont représenté en 2024 un quart des événements signalés portés à la connaissance de l'Agence. Le reliquat des événements concernait 300 signalements recouvrant un impact mineur pour l'entité victime, sans avoir identifié d'intrusion dans le système d'information (hameçonnage, déni de service, etc.). Les typologies de victimes les plus représentées dans les événements de sécurité numérique rapportés sur l'année 2024 sont les PME/TPE/ETI (37 %) tous secteurs d'activité confondus, ainsi que les collectivités territoriales (29 %). Au cours de l'année 2024, dans le cadre de ces échanges, l'ANSSI a signalé aux CSIRT territoriaux 102 événements de sécurité numérique survenus au sein de leur territoire. Elle les a par ailleurs accompagné dans leur montée en maturité et a œuvré à promouvoir leur visibilité au sein de l'écosystème de la cybersécurité nationale. 2024 a notamment été marquée par le renforcement de la synchronisation opérationnelle du CERT-FR avec les CSIRT territoriaux. Ces derniers ont également été intégrés dans le serveur vocal interactif du CERT-FR. Enfin, sur l'année 2024, l'Agence a soutenu la création de trois Centres de Ressources Cyber dans les DROM-COM (à la Réunion, dans les territoires français d'Amérique et en Nouvelle-Calédonie). Leur ouverture au cours du dernier trimestre 2024 leur a permis de traiter de premiers incidents. Une vision consolidée des 15 CSIRT territoriaux et CRC (Centres de Ressources Cyber) en France métropolitaine et ultramarine pourra être apportée dès l'année 2025.

On compte aujourd'hui quinze CSIRT territoriaux et CRC implantés :

- en Bourgogne-Franche-Comté avec le CSIRT Bourgogne-Franche-Comté ;
- en Bretagne avec Breizh Cyber ;
- en Centre-Val de Loire avec CybeRéponse ;
- en Corse avec le CSIRT CyberCorsica | Centre de cybersécurité de Corse ;
- en Grand-Est avec Grand-Est Cybersécurité ;
- en Hauts-de-France avec le CSIRT Hauts-de-France ;
- en Île-de-France avec Urgence Cyber Île-de-France ;
- en Normandie avec Normandie Cyber ;
- en Nouvelle-Aquitaine avec le Campus régional de Cybersécurité et de Confiance numérique ;
- en Occitanie avec Cyber'Occ ;
- en Pays de la Loire avec Pays de la Loire Cyber Assistance ;
- en région Sud Provence-Alpes-Côte-d'Azur avec Urgence Cyber région Sud ;
- dans les territoires français d'Amérique (Région Guadeloupe, la collectivité territoriale de Guyane, les collectivités d'Outre-mer de Saint-Martin, Saint-Barthélemy et Saint-Pierre et Miquelon) avec le CSIRT-ATLANTIC ;
- à La Réunion avec le CSIRT La Réunion ;
- en Nouvelle-Calédonie avec le Centre Cyber du Pacifique.

Comme pour les CSIRT territoriaux, la montée en puissance des CSIRT ministériels est encadrée et soutenue par l'Agence, qui accompagne leur autonomisation dans le domaine des capacités de détection et de supervision, tout en demeurant garante d'une détection interministérielle efficace. En 2024, un Comité technique commun au CERT-FR et aux CSIRT ministériels a été mis en place. Débutée en janvier 2024, l'incubation des 10 principaux CSIRT ministériels a pris fin en avril, actant leur montée en maturité. Les échanges opérationnels ont d'ores et déjà débuté et ont vocation à se renforcer. En effet, le CERT-FR reçoit des remontées de signalement d'incidents de leur part et partage des marqueurs sur la menace à intervalle régulier. ●

« Les CSIRT relais sont des acteurs clés pour simplifier le parcours des usagers et le rendre accessible à tous. Ils permettent un accompagnement humain, personnalisé, ancré dans la réalité locale et sectorielle. »

Jeanne Fournis, cheffe de projet, sous-direction Opérations

Une offre de services coconstruite pour démultiplier l'accompagnement cyber

Pour accompagner un nombre toujours plus important de bénéficiaires, l'ANSSI repense en continu ses modes de travail et ses outils. L'année 2024 a été riche en développements et déploiements de services numériques en partenariat avec des acteurs clés de l'écosystème cyber, activité qui se poursuivra et s'intensifiera en 2025. L'offre de services se décline ainsi en plusieurs plateformes qui s'inscrivent dans un changement d'échelle nécessaire à la mise en œuvre de la directive NIS 2. Elles permettent de démultiplier les actions de l'Agence et de porter ses messages au plus près de chaque bénéficiaire.

MonAideCyber est un dispositif qui fédère une communauté d'aidants cyber afin qu'ils puissent accompagner au mieux leurs bénéficiaires dans leurs démarches de renforcement de cybersécurité. Cette communauté des « aidants cyber » inclut notamment des représentants des services de l'État – police, gendarmerie, douanes, Direction Générale de la Sécurité Intérieure (DGSI), Direction du renseignement et de la sécurité de la Défense (DRSD), préfectures, etc. – d'administrations, de collectivités territoriales, de groupements d'intérêt public, de chambres consulaires et syndicales, d'associations – campus cyber, opérateurs publics de services numériques (OPSN), associations sectorielles, numériques ou de développement économique. Gratuite, cette innovation de l'Agence est soutenue par le ministère de l'Intérieur, *Cybermalveillance.gouv.fr* et la CNIL. Après une phase d'expérimentation de deux ans, MonAideCyber a été déployé nationalement tout en poursuivant la construction de nouvelles fonctionnalités qui prennent en compte les retours des utilisateurs. Plus de 1000 aidants cyber sont déjà référencés et MonAideCyber comptait à ce jour plus de 1450 « aidés » fin 2024.

Dans la même perspective de pédagogie et avec l'objectif de fournir un service « clé en main », l'ANSSI a poursuivi en 2024, en collaboration avec la CNIL, l'accélération de MonServiceSécurisé. Cette plateforme, disponible depuis 2022, est une innovation de l'Agence développée conformément aux principes de la méthode BetaGouv. Destinée à aider simplement les entités publiques (communes, communautés de communes, agglomérations, métropoles, opérateurs publics de services numériques (OPSN),

« Il est important de ne pas attendre la transposition de la directive NIS 2 pour aider les entités concernées à se protéger. Pour cela, l'ANSSI innove avec ses bénéficiaires et mobilise notamment des méthodes issues du design pour proposer des solutions adaptées à leurs besoins. »

Solène Bellego, responsable design au sein du Laboratoire d'innovation, sous-direction Stratégie

1 501
diagnostics réalisés

1 487
aidants cyber référencés sur MonAideCyber

syndicats mixtes, conseils départementaux, universités, ministères) à sécuriser leurs services en ligne, elle accélère l'homologation de sécurité et facilite la mise en conformité des entités publiques avec la réglementation. En 2024, le nombre d'utilisateurs a atteint 6 063, soit une augmentation de 100 % en un an, pour 3 403 services sécurisés. Au cours de l'année écoulée, MonServiceSécurisé a ainsi permis de corriger 81 986 vulnérabilités pour ces entités utilisatrices. La plateforme a par ailleurs été lauréate en 2024, pour la deuxième fois, du fonds d'accélération des start-up d'État de la Direction interministérielle du numérique.

Également destinée aux agents de la fonction publique et complémentaire aux mesures de sécurité mises en place par les ministères, la plateforme *jecliqueoupas.cyber.gouv.fr* a été développée par la société Glimps dans le cadre d'un marché public piloté par l'ANSSI, et mise en service en 2024. Solution dédiée à l'analyse de fichiers permettant d'évaluer rapidement et facilement la dangerosité de n'importe quel document reçu, Jecliqueoupas constitue une alternative à des services librement accessibles en ligne, fournis par des sociétés étrangères dont l'utilisation des données collectées n'est pas maîtrisée.

En 2024, *monespacenis2.cyber.gouv.fr* a également vu le jour en version bêta, développé par l'Agence et s'adressant à toutes les entités souhaitant savoir si elles sont concernées par la directive NIS 2. La plateforme leur permet d'effectuer un test afin de le déterminer, et de savoir à quelle catégorie (essentielle ou importante) elles appartiennent si elles le sont. Le service permet également de s'informer sur les exigences de la directive et de s'inscrire à une newsletter dédiée.

D'autres produits sont venus compléter l'offre de services de l'Agence en 2024. Issues d'une collaboration entre l'ANSSI et l'InterCERT France, des fiches réflexes ont été mises à disposition sur le site web du CERT-FR, *cert.ssi.gouv.fr*. Ces livrables sont ainsi pensés pour aider les équipes de détection et ou de réponse à incident à réagir de manière efficace face aux incidents de sécurité. L'objectif est de fournir des ressources concises et opérationnelles pour renforcer la préparation et la réactivité des équipes face aux menaces numériques.Des contributions en *open source* sur GitHub ont également été effectuées, s'inscrivant dans une dynamique de partage des outils de l'ANSSI (outils d'investigation numérique, d'audits automatisés ou de sécurisation des systèmes d'information) au sein de la communauté des professionnels de la cybersécurité (CSIRT, équipes et prestataires de sécurité, etc.) ●

81 986
vulnérabilités corrigées

3 403
services sécurisés grâce à MonServiceSécurisé

↘ AlerteCyber en lien avec *cybermalveillance.gouv.fr* : un dispositif pour alerter les entités de toutes tailles

Le dispositif AlerteCyber, lancé en juillet 2021, à l'initiative du GIP ACYMA et d'un collectif d'organisations professionnelles, a pour objectif d'accompagner les entités de toutes tailles face à la menace, de les informer et de les inciter à prendre les mesures qui s'imposent pour se protéger. Le dispositif AlerteCyber est lancé dès lors qu'une menace ou une faille sérieuse est identifiée et qualifiée en tant que telle, conjointement par l'ANSSI et *cybermalveillance.gouv.fr*. Il vise plus particulièrement des solutions matérielles ou logicielles déployées par le public ciblé par le GIP, utilisées principalement par des particuliers ou des structures ne disposant pas d'un système d'information en tant que tel, type TPE ou petite collectivité territoriale. En 2024, deux campagnes AlerteCyber ont été émises :

→ 26 février : Faille de sécurité critique dans Microsoft Outlook
→ 6 mai : Failles de sécurité critiques dans les produits QNAP

Face à l'accroissement des vulnérabilités identifiées par l'ANSSI, ce dispositif fait preuve de son efficacité pour répondre à l'enjeu de prévention des attaques et d'information des victimes. ●

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 place par l'ANSSI pour l'année 2024. 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 du secret des correspondances,
- → préservation de la sécurité des réseaux 5G et des générations futures.

L'année 2024 a été marquée par l'entrée en vigueur des nouvelles dispositions opérationnelles de la LPM 2024-2030 rendues effectives sur le plan juridique grâce à la publication des décrets et arrêtés d'application.

Un premier jeu de capacités avait été offert par la précédente LPM et avait été mis en œuvre, en particulier pour identifier des victimes de cyberattaques. En 2024, l'ANSSI a su implémenter un premier dispositif efficient sous le contrôle de l'ARCEP et de la CNIL en amont des JOP. Les travaux visant à mettre en œuvre pleinement les capacités d'action additionnelles offertes par la nouvelle LPM progressent en lien avec l'ensemble des acteurs publics et privés concernés. Ces capacités permettront, à terme, la prévention et la caractérisation de la menace (filtrage DNS, collecte de cache DNS, recueil de données) et un meilleur traitement des vulnérabilités produit en obligeant notamment l'éditeur à notifier les vulnérabilités significatives à l'Agence et à ses clients.

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 2024

En 2024, l'Agence a été destinataire de 236 signalements au titre de l'article L.2321-4 du code de la défense. La moitié (49 %) 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 37 % des signalements. Seuls 11 % des signalements reçus par l'ANSSI ont trait à des vulnérabilités affectant des logiciels, généralement des solutions professionnelles.

À ce jour, l'Agence n'a jamais été confrontée à un déclarant qui ne soit pas considéré comme de bonne foi et n'a donc procédé à aucune déclaration au parquet dans le cadre de ce dispositif.

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 susceptible de recueillir et de traiter des signalements émis par les lanceurs d'alerte 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.

L'ANSSI a été désignée par ce décret comme autorité susceptible 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 (SSI) 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)[16] ;
- → non-respect du cadre réglementaire en matière de qualification et de certification de produits ou services ;
- → violation d'un contrôle réglementaire[17], 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[18], 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 2024

Aucun signalement en lien avec un non-respect des dispositifs réglementaires en matière de sécurité des systèmes d'information n'a été reçu par l'ANSSI. ●

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

[17] 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).

[18] 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, pour transmettre des messages de signalement de vulnérabilités ou de compromissions auprès d'abonnés concernés.

BILAN 2024

En 2024, neuf campagnes de signalement de vulnérabilités représentant 15 900 adresses IP ont été menées auprès des abonnés des opérateurs. 8 731 d'entre elles ont pu être identifiées. L'ensemble des OCE concernés a participé à l'ensemble des campagnes.

Le site *cybermalveillance.gouv.fr* héberge la page d'alerte vulnérabilité vers laquelle les opérateurs redirigent leurs clients dans le cadre de ces campagnes, permettant de mesurer le suivi de ces dernières. Ainsi, 438 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

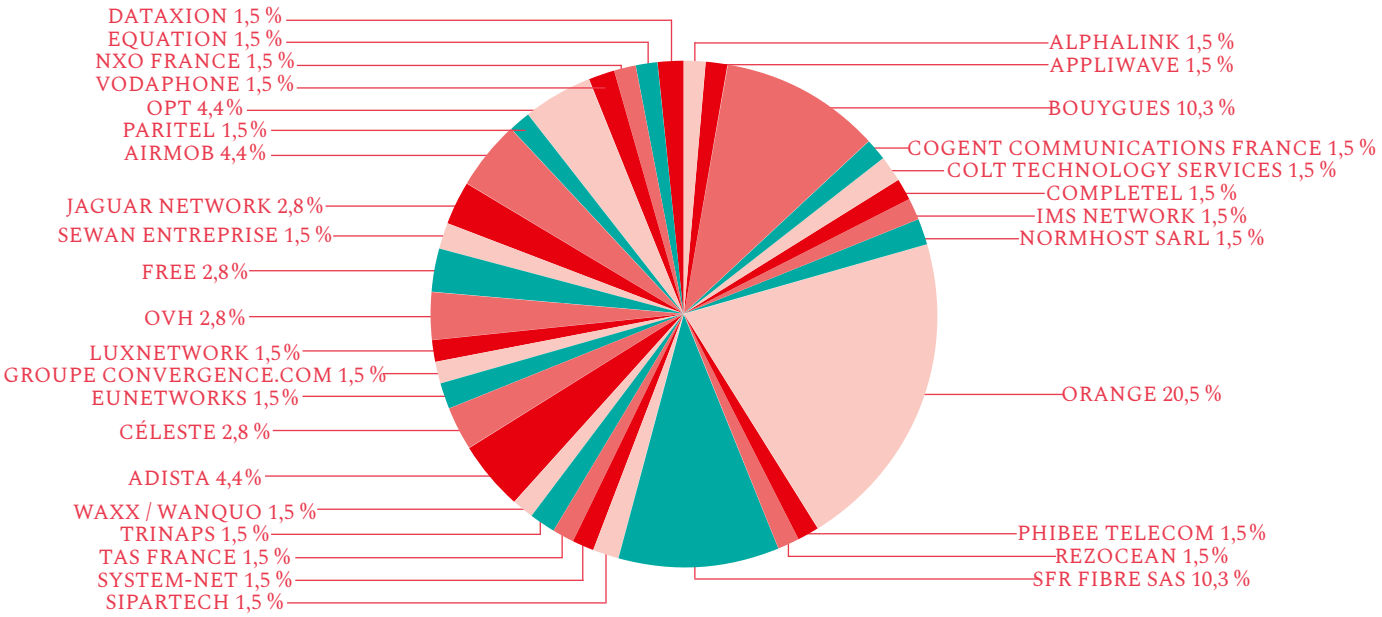
Cet article précise dans quels cas l'ANSSI peut demander des informations aux OCE. L'alinéa premier prévoit que, pour les besoins de la sécurité des systèmes d'information d'un opérateur d'importance vitale (OIV), d'un opérateur de service essentiel (OSE) ou d'une autorité publique, l'Agence peut demander 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 2024

En 2024, 68 demandes d'identification pour un total de 978 adresses IP ont été effectuées par l'ANSSI auprès de 34 opérateurs de communications électroniques. Orange, SFR et Bouygues étant les principaux fournisseurs des OIV, OSE et autorités publiques, ils concentrent à eux trois près de la moitié des demandes.

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



© L'article L2321-4-1 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 L2321-4-1 du code de la défense nationale a été créé par la LPM 2024-2030. Il crée une nouvelle obligation à la charge des éditeurs : la déclaration des vulnérabilités significatives à l'ANSSI et à ses 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 nouvelle 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.

Cette nouvelle obligation s'applique lorsque les conditions suivantes sont réunies[19] :

- La vulnérabilité concerne un éditeur de logiciel : au sens de la loi, on entend par éditeur de logiciel « toute personne physique ou morale qui conçoit ou développe un produit logiciel ou fait concevoir ou développer un produit logiciel et qui le met à la disposition d'utilisateurs, à titre onéreux ou gratuit ».
- L'éditeur fournit son logiciel :

[19] Une foire aux questions est disponible sur le site de l'ANSSI : *https://cyber.gouv.fr/sites/default/files/document/FAQ_decret_LPM-2024-2030_consultations.pdf*

- Sur le territoire français ;
  → À des sociétés ayant leur siège social sur le territoire français ;
  → Ou à des sociétés contrôlées, au sens de l'article L. 233-3 du code de commerce, par des sociétés ayant leur siège social sur le territoire français.
- La vulnérabilité qui affecte le logiciel est significative : le caractère significatif est évalué par l'éditeur en fonction de sa connaissance du logiciel, de ses utilisateurs, de son usage et de son environnement, en s'appuyant notamment sur les critères proposés par l'article R2321-1-16 du code de la défense :
  → Le nombre d'utilisateurs concernés par la vulnérabilité ou l'incident affectant le produit ;
  → Le nombre de produits intégrant le produit affecté ;
  → L'impact technique, potentiel ou actuel, de la vulnérabilité ou de l'incident sur le fonctionnement attendu du produit. Selon les fonctionnalités du produit, cet impact est évalué au regard de critères de sécurité tels que la disponibilité, l'intégrité, la confidentialité ou la traçabilité ;
  → Le type de produit au regard de ses usages et de l'environnement dans lequel il est déployé ;
  → L'exploitation imminente ou avérée de la vulnérabilité ;
  → L'existence d'une preuve technique d'exploitabilité ou d'un code d'exploitation.

BILAN 2024

Depuis son entrée en vigueur le 1er juin 2024, l'ANSSI a traité une vulnérabilité significative entrant dans le champ d'application de l'article L.2321-4-1 du code de la défense nationale. ●

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 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 2024

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 2024 sur la base de ces capacités.

À la suite de la publication du décret 2024-421 du 10 mai 2024, ce dispositif s'impose désormais aux OCE ayant le statut d'opérateur d'importance vitale, et fait également l'objet de compensations financières pour le déploiement des dispositifs de détection. L'Agence s'appuie sur le commissariat aux communications électroniques de défense (CCED) pour assurer le déploiement de capacités permettant de mieux répondre aux besoins des opérateurs pour remplir la mission confiée par la loi. ●

Ⓑ L'ANSSI peut mettre un 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 de 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, étroitement contrôlé par l'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 2024

En 2024, quatre opérations ont été lancées auprès d'hébergeurs et deux opérations initiées en 2023 ont été prorogées 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.

L'année a notamment été marquée par des travaux internes et avec les hébergeurs afin d'opérationnaliser les nouvelles capacités octroyées par la LPM 2024-2030. Ceci a conduit en fin d'année à la première opération de recueil de données tel que permis par l'extension des capacités de la LPM. ●

Ⓒ 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 nouvelle 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. 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 2024

Des échanges ont été engagés auprès des différents opérateurs de communications électroniques pour permettre la mise en œuvre de cette mesure. Une première preuve de concept a été réalisée avec un OCE, toutefois cette mesure demande des aménagements importants au sein des infrastructures des opérateurs et de l'Agence. Aussi, des échanges ont été initiés avec le CCED afin de permettre ces adaptations techniques. ●

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 2024

L'Agence a pu développer une capacité de blocage et de redirection de nom de domaine avant les JOP de Paris 2024 grâce à la coopération des principaux OCE et du ministère de l'Intérieur. L'ANSSI s'appuie sur la plateforme d'échange mise en place par le ministère qui permet d'automatiser l'envoi d'ordres de blocage et de déblocage auprès des opérateurs. La mutualisation de cette plateforme a permis de réaliser d'importantes économies de moyens humains et financiers pour la mise en œuvre de cette mesure. ●

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.

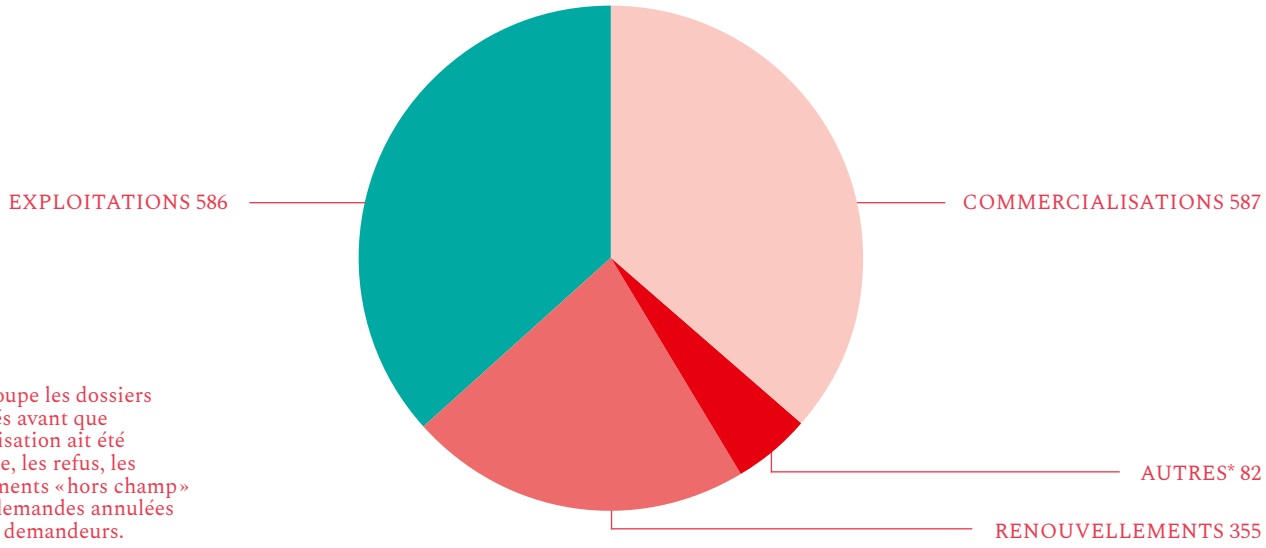
La demande d'autorisation est instruite par les services de l'Agence, qui s'assurent en particulier que le dispositif correspond à un usage légitime prévu par le droit français, qu'il est adéquatement sécurisé et n'est pas détournable de son usage légitime. Elle est ensuite étudiée par une commission 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 2024

L'ANSSI a rendu 1610 décisions en 2024, dont 52 décisions de refus. Les volumes d'autorisations de commercialisation (à l'intention des fabricants) et d'autorisations de détention (destinées aux exploitants) sont assez proches puisque ces deux types d'autorisation vont généralement de pair. ●

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[20].

Ce dispositif, dont la mise en œuvre relève du secrétariat général de la défense et de la sécurité nationale, 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 2024

Les décisions relatives aux antennes 5G

Pour l'année 2024, 83 décisions ont été rendues, dont trois 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, 39 autorisations ont été délivrées pour des cœurs de réseau de cinquième génération. ●

[20] 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

DevSecOps, version 1.0.
En savoir plus

Virtualisation, version 1.0.
En savoir plus

→ LES BACK TO BASICS (version anglaise des Essentiels)

DevSecOps, version 1.0.
En savoir plus

Distributed Denial of Service (DDoS), version 2.0.
En savoir plus

Secure implementation of CMS, version 1.1.
En savoir plus

Virtualization, version 1.0.
En savoir plus

The golden rules of backup, version 1.1.
En savoir plus

→ LES FONDAMENTAUX

Sécurisation d'une infrastructure VMware, version 1.0.
En savoir plus

→ LES GUIDES TECHNIQUES

Recommandations pour les architectures des interconnexions multiniveaux, version 1.0.
En savoir plus

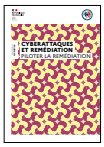
Recommandations relatives aux architectures des services DNS, version 1.0.
En savoir plus

Recommandations pour l'hébergement des SI sensibles dans le cloud, version 1.0.
En savoir plus

Recommandations de déploiement d'un service IAAS OpenStack SecNumCloud, version 1.0.
En savoir plus

Recommandations de sécurité pour un système d'IA générative, version 1.0.
En savoir plus

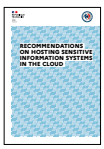
Cyberattaques et remédiation : La remédiation du Tier 0 Active Directory, version 1.0.
En savoir plus



Cyberattaques et remédiation : Piloter la remédiation, version 1.0.
En savoir plus

Cyberattaques et remédiation : Les clés de décision, version 1.0.
En savoir plus

Security recommendations for a generative AI system, version 1.0.
En savoir plus



Recommendations on hosting sensitive information systems in the cloud, version 1.0.
En savoir plus

PUBLICATIONS SCIENTIFIQUES

→ ARTICLES SCIENTIFIQUES PRÉSENTÉS EN CONFÉRENCE

Laboratoire cryptologie

A Not So Discrete Sampler: Power Analysis Attacks on HAWK signature scheme, Morgane Guerreau and Mélissa Rossi [⋄]. CHES 2024, vol. 4, pp. 156-178.
En savoir plus

A Univariate Attack against the Limited-Data Instance of Ciminion, Augustin Bariant [⋄]. Selected Areas in Cryptography (SAC) 2024.
En savoir plus

Fast AES-Based Universal Hash Functions and MACs, Augustin Bariant, Jules Baudrin, Gaëtan Leurent, Clara Pernot, Léo Perrin, et Thomas Peyrin. IACR Transactions on Symmetric Cryptology (ToSC) 2024, vol. 2, pp. 35-67.
En savoir plus

G+G : A Fiat-Shamir Lattice Signature Based on Convolved Gaussians, Julien Devevey [⋄], Alain Passelègue and Damien Stehlé. Asiacrypt 2024, pp. 37-64.
En savoir plus

HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures, Jung Hee Cheon, Hyeongmin Choe, Julien Devevey, Tim Güneysu, Dongyeon Hong, Markus Krausz, Georg Land, Marc Möller, Damien Stehlé, et Minjune Yi. TCHES 2024, pp. 25-75.
En savoir plus

Quarantined-TreeKEM: a Continuous Group Key Agreement for MLS, Secure in Presence of Inactive Users, Céline Chevalier, Guirec Lebrun, Ange Martinelli and Abdul Rahman Taleb. ACM CCS 2024.
En savoir plus

Raccoon : A Masking-friendly Signature Proven in the Probing Model, Rafaël del Pino, Shuichi Katsumata, Thomas Prest and Mélissa Rossi [⋄]. CRYPTO 2024, pp. 409-444.
En savoir plus

The Algebraic FreeLunch: Efficient Gröbner Basis Attacks Against Arithmetization-Oriented Primitives, Augustin Bariant [⋄], Aurélien Boeuf, Axel Lemoine, Irati Manterola Ayala, Morten Øygarden, Léo Perrin et Håvard Raddum. CRYPTO 2024, pp. 139-173.
En savoir plus

Updatable Encryption from Group Actions, Antonin Leroux and Maxime Roméas [⋄]. PQCrypto 2024, vol. 2, pp. 20-53.
En savoir plus

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

Laboratoire de la sécurité des technologies sans-fil

Time-Memory Trade-Offs Sound the Death Knell for GPRS and GSM, Gildas Avoine, Xavier Carpent, Tristan Claverie [⋄], Christophe Devine [⋄], Diane Leblanc-Albarel, conférence CRYPTO 2024, Santa Barbara, 206-240.

Communications à grande distance avec un lecteur ISO 14443, Yoann Burny, Pierre-Michel Ricordel [⋄], SSTIC 2024, Rennes.
En savoir plus

Laboratoire exploration et recherche en détection

Inductive Lateral Movement Detection in Enterprise Computer Networks, Corentin Larroche, ESANN 2024.
En savoir plus

Laboratoire sécurité réseau, protocole

A Unified Symbolic Analysis of WireGuard, Pascal Lafourcade, Dhekra Mahmoud et Sylvain Ruhault [⋄]. NDSS 2024.
En savoir plus

Laboratoire architecture matérielle et logicielle

Characterizing and Modeling Synchronous Clock-Glitch Fault Injection, Amélie Marotta, Ronan Lashermes, Guillaume Bouffard [⋄], Olivier Sentieys et Rachid Dafali, COSADE 2024.
En savoir plus

Évolutions dans la sécurité des modules de gestion de l'énergie, Gwenn Le Gonidec, Maria Méndez Real, Guillaume Bouffard [⋄] et Jean-Christophe Prévotet, JAIF 2024.
En savoir plus

Évolution des protections du moteur Javascript V8, François Jolivet [⋄]. SSTIC' 24,
En savoir plus

Laboratoire sécurité des composants

Butterfly Probes : Estimating the Derivative of the Magnetic Flux, Philippe Maurine, Jérémy Raoult, Anselme Mouette, Julien Toulemont [⋄]. EMC COMPO 2024.
En savoir plus

Laboratoire cryptologie, laboratoire exploration et recherche en détection et laboratoire sécurité des composants

Retour d'expérience sur l'organisation d'un CTF, Adrien Thuau, Alexandre Iooss [⋄], Emilien Court, Jérémy Jean, Matthieu Olivier, Tristan Claverie [⋄]. SSTIC 2024.
En savoir plus

→ ARTICLES PUBLIÉS DANS DES JOURNAUX DE RECHERCHE SCIENTIFIQUE

Laboratoire cryptologie

Masking the GLP Lattice-Based Signature Scheme at Any Order, Gilles Barthe, Sonia Belaïd, Thomas Espitau, Pierre-Alain Fouque, Benjamin Grégoire, Mélissa Rossi, Mehdi Tibouchi. Journal of Cryptoly 2024.

A Long Tweak Goes a Long Way : High Multi-User Security Authenticated Encryption from Tweakable Block Ciphers, 2. Benoit Cogliati, Jérémy Jean, Thomas Peyrin et Yannick Seurin, IACR Communications in Cryptology 2024, vol. 1.

A provably masked implementation of the BIKE Key Encapsulation Mechanism, Loïc Demange, Mélissa Rossi. Communications in Cryptology 2024, vol. 1, Number 1.

→ CONTRIBUTIONS À DES OUVRAGES SCIENTIFIQUES

Laboratoire de la sécurité des technologies sans-fil

Sécurité électromagnétique : panorama des modèles de menace, José Lopes Esteves [⋄], magazine *MISC*, hors-série n° 29.

An Introduction to intentional electromagnetic interference exploitation, José Lopes Esteves [⋄], Embedded Cryptography, éditions ISTE/WILEY.

PUBLICATIONS OPEN SOURCE

Laboratoire exploration et recherche en détection

DECODE : outil de détection de fichier Portable Executable (PE) malveillant basé sur les données NTFSInfo collectées par l'outil DFIR-ORC.
En savoir plus

Laboratoire sécurité des composants

Hackropole-hugo : moteur du site hackropole.fr, utilisé pour héberger les archives des challenges du French CyberSecurity Challenge (FCSC).
En savoir plus

Laboratoire d'architectures matérielles et logicielles

Chipsec-check : génération de clé USB incluant chipsec et d'autres outils pour tester des exigences de sécurité matérielle et firmware.
Code source Github

Keysas : un prototype de station de décontamination de fichiers avec un focus sur la sécurité de la station elle-même.
Code source Github

Lidi : diode logicielle développée en Rust initiée par le LSL et maintenue par le LAM.
Code source Github

CONTRIBUTIONS À DES PROJETS OPEN SOURCE TIERS

Laboratoire sécurité des composants

QEMU : émulateur générique et machine virtuelle ; contribution dans les plugins TCP.
En savoir plus

PicoEMP : injecteur de fautes électro-magnétiques (EM-FI) ; correction d'un bug.
Code source Github

CTFd : gestion d'un challenge Capture-The-Flag (CTF) en ligne ; contribution suite au FCSC.
Code source Github

Laboratoire sécurité des technologies sans-fil

Tamarin prover : modèles Tamarin des protocoles d'établissement de clé en Bluetooth, Bluetooth Low Energy et Bluetooth Mesh.
Code source Github

Laboratoire d'architectures matérielles et logicielles

Chipsec : Platform Security Assessment Framework (Intel). Mainteneur pour l'architecture AMD, ajout de support pour la construction d'images USB.
Code source Github

Noyau Linux : multiples corrections de vulnérabilités.
Corruption mémoire, confusion de types

Systemd : correction du comportement de l'*enrollment* des clés secure-boot par bootctl afin de respecter la spécification UEFI.
Contribution publique

RAPPORTS SUR LES MENACES ET INCIDENTS

Panorama de la cybermenace 2023, 27 février 2024.
En savoir plus

Cyber Threat Overview 2023, 27 février 2024.
En savoir plus

État de la menace ciblant les grands événements sportifs en France, 17 avril 2024.
En savoir plus

Opération ENDGAME, 30 mai 2024.
En savoir plus

Failles sur les équipements de sécurité – Retour d'expérience du CERT-FR, 12 juin 2024.
En savoir plus

Malicious activities linked to the Nobelium intrusion set, 19 juin 2024.
En savoir plus

Codes malveillants utilisés à des fins destructrices, 11 juillet 2024.
En savoir plus

État de la menace ciblant les organismes de recherche et think tanks, 02 septembre 2024.
En savoir plus

Exfiltration de données du secteur social – Retour d'expérience du CERT-FR, 24 septembre 2024.
En savoir plus

État de la menace ciblant le secteur de la santé, 07 novembre 2024.
En savoir plus

État de la menace ciblant le secteur de l'eau, 28 novembre 2024.
En savoir plus

PARTENARIATS

Position Paper on Quantum Key Distribution.
En savoir plus

Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography.
En savoir plus

ÉTUDES DE MARCHÉ

État de l'offre des solutions de cryptographie post-quantique en 2023, version 1.0.
En savoir plus

État de l'offre de prestation d'accompagnement et de conseil en sécurité, version 1.0.
En savoir plus

Observatoire des métiers, L'attractivité et la représentation des métiers de la cybersécurité vues par les professionnels, version 1.0.
En savoir plus

RÉFÉRENTIELS

Prestataires d'audit de la sécurité des systèmes d'information - Référentiel d'exigences Version 2.2 du 1er août 2024 (publié le 29/11/24)

Prestataires de réponse aux incidents de sécurité - Référentiel d'exigences Version 3.0 du 28 juillet 2024 (publié le 29/11/2024)

Version 1.0 – Avril 2025
Dépôt légal : avril 2025
ISSN 2804-0031 (imprimé)
ISSN 2804-5920 (en ligne)
Licence Ouverte/Open
Licence (Etalab — V1)

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